

THE LARGE DAVENPORT CONSTANT I: GROUPS WITH A CYCLIC, INDEX 2 SUBGROUP

ALFRED GEROLDINGER AND DAVID J. GRYNKIEWICZ

ABSTRACT. Let G be a finite group written multiplicatively. By a sequence over G , we mean a finite sequence of terms from G which is unordered, repetition of terms allowed, and we say that it is a product-one sequence if its terms can be ordered so that their product is the identity element of G . The *small Davenport constant* $d(G)$ is the maximal integer ℓ such that there is a sequence over G of length ℓ which has no nontrivial, product-one subsequence. The *large Davenport constant* $D(G)$ is the maximal length of a minimal product-one sequence—this is a product-one sequence which cannot be factored into two nontrivial, product-one subsequences. It is easily observed that $d(G) + 1 \leq D(G)$, and if G is abelian, then equality holds. However, for non-abelian groups, these constants can differ significantly. Now suppose G has a cyclic, index 2 subgroup. Then an old result of Olson and White (dating back to 1977) implies that $d(G) = \frac{1}{2}|G|$ if G is non-cyclic, and $d(G) = |G| - 1$ if G is cyclic. In this paper, we determine the large Davenport constant of such groups, showing that $D(G) = d(G) + |G'|$, where $G' = [G, G] \leq G$ is the commutator subgroup of G .

1. INTRODUCTION AND MAIN RESULT

Let G be a multiplicatively written, finite group. A sequence S over G means a finite sequence of terms from G which is unordered, repetition of terms allowed. We say that S is a product-one sequence if its terms can be ordered so that their product equals 1, the identity element of the group. The *small Davenport constant* $d(G)$ is the maximal integer ℓ such that there is a sequence over G of length ℓ which has no nontrivial, product-one subsequence. The *large Davenport constant* $D(G)$ is the maximal length of a minimal product-one sequence—this is a product-one sequence which cannot be partitioned into two nontrivial, product-one subsequences. A simple argument shows that $d(G) + 1 \leq D(G) \leq |G|$.

The problem of finding the precise value of the Davenport constant and what is now known as the Erdős–Ginzburg–Ziv Theorem became the starting points of Zero-Sum Theory. Since that time (dating back to the early 1960s), it has developed into a flourishing branch of Additive and Combinatorial Number Theory. We briefly discuss some of the motivation for these problems. For more detailed information, we defer to the surveys [5, 9, 12] or the monographs [14, 17]. Apart from abelian groups, the Davenport constant has also been studied for finite abelian (non-cancellative) semigroups (see [29], [14, Proposition 2.8.13]).

Although the main focus of Zero-Sum Theory has been on abelian groups, research was never restricted to the abelian setting alone. To provide one example apart from the Davenport constant, let $E(G)$ denote the smallest integer ℓ guaranteeing that every sequence S over G of length $|S| \geq \ell$ has a product-one

2010 *Mathematics Subject Classification*. 20D60, 11B75, 13A50.

Key words and phrases. zero-sum sequence, product-one sequence, Davenport constant, Noether bound.

This work was supported by the *Austrian Science Fund FWF* (Project No. P21576-N18).

subsequence of length $|G|$. Motivated by the classical Erdős–Ginzburg–Ziv Theorem, the study of $E(G)$ has attracted much attention for non-abelian groups [31, 2, 11, 10]. In all cases studied so far (abelian and non-abelian), it has turned out that $E(G) = |G| + d(G)$.

If G is a finite abelian group, then an easy observation shows that $d(G) + 1 = D(G)$. Here there is no difference between the combinatorially defined small davenport constant $d(G) + 1$ and the monoid theoretic large Davenport Constant $D(G)$. In this classical setting, the Davenport constant was first introduced by Rogers [27] (though Davenport became more famous for promoting it) who pointed out a connection between $D(G)$ and irreducible elements in a ring of algebraic integers with ideal class group isomorphic to G (see Section 2). His observation was deepened by Narkiewicz [22] whose paper was the first step in the creation of a strong bridge between the arithmetic of Krull monoids and Additive Combinatorics (via the associated monoid of zero-sum sequences over the class group; see [12] for a survey).

The first attempts to study a Davenport constant in a non-abelian setting were carried out by Olson and White [26], who defined the small Davenport constant of a non-abelian group and gave a general upper bound that was shown to be tight for groups having a cyclic, index 2 subgroup; see Theorem 3.1. However, the definition of the small Davenport constant is not as fully satisfying in this setting. The first reason for this is simple: there is no monoid factorization interpretation of the small Davenport constant over a non-abelian group. The second reason for this regards Invariant Theory and the Noether constant.

Let G be a finite group, let \mathbb{F} be a field whose characteristic does not divide $|G|$, and let $\beta(G)$ denote the Noether constant, which is defined as the maximal degree of an invariant polynomial in a minimal generating set of the invariant ring $\mathbb{F}[V]^G$. When G is abelian, we have $d(G) + 1 = D(G)$. However, when G is non-abelian, there are examples where $d(G) + 1 < \beta(G)$, meaning the small Davenport constant cannot be used for bounding $\beta(G)$ from above. Attempting to rectify this problem, we have defined the large Davenport constant simply by taking the natural monoid theoretic definition and extending it to non-abelian groups. The natural conjecture is that $d(G) + 1 \leq \beta(G) \leq D(G)$ might hold for groups in general. By the results of the present paper, this conjecture holds for all groups having a cyclic, index 2 subgroup. For more on invariant theory and the Noether constant, we refer the reader to the monographs [25, 24] or to more recent work [23, 15].

Our main result is the following theorem, in which we parallel the early result of Olson and White [26] that determined the small Davenport constant of a finite group having a cyclic, index 2 subgroup, by instead determining the large Davenport constant for all such groups. Theorem 1.1 covers dihedral groups, semi-dihedral groups, and generalized quaternion or dicyclic groups, as well as many more. Building upon the results of this paper, we will give more general upper bounds for $D(G)$ in a sequel [16].

Theorem 1.1. *Let G be a finite group having a cyclic, index 2 subgroup. Then*

$$D(G) = d(G) + |G'| \quad \text{and} \quad d(G) = \begin{cases} |G| - 1 & \text{if } G \text{ is cyclic} \\ \frac{1}{2}|G| & \text{if } G \text{ is non-cyclic,} \end{cases}$$

where $G' = [G, G] \leq G$ is the commutator subgroup of G .

The paper is divided as follows. In Section 2, we introduce and adapt notation used for sequences and sumsets over abelian groups and prove several basic facts. In Section 3, we give some general upper bounds that can be used in conjunction with inductive arguments. Section 4 deals entirely with classical

results for abelian groups, needed for later proofs, and the proof of one axillary lemma needed for handling dicyclic groups. The main bulk of the proof of Theorem 1.1 is then carried out in Section 5, beginning with an overview of the possible isomorphism classes of groups having a cyclic, index 2 subgroup.

2. NOTATION AND PRELIMINARIES

All intervals will be discrete, so for real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. If A and B are sets, then whenever addition or multiplication between elements of A and B is allowed, we define their sumset and product-set as

$$A + B = \{a + b : a \in A, b \in B\} \quad \text{and} \quad AB = \{ab : a \in A, b \in B\}.$$

Of course, we use the abbreviations $A + g = \{a + g : a \in A\}$, $Ag = \{ag : a \in A\}$ and $gB = \{gb : b \in B\}$ when dealing with a single element g for which the respective addition or multiplication is defined.

In our main applications, all groups will be finite, but we will encounter groups written both additively and multiplicatively, reserving addition only for cases where it is a commutative operation. For the moment, assume that G is a group written multiplicatively except when otherwise noted.

If $A \subset G$ is a nonempty subset, then we use $\langle A \rangle \leq G$ to denote the subgroup generated by A and use $H(A) := \{g \in G : gA = A\}$ to denote the left *stabilizer* of A . Then $H(A) \leq G$ is a subgroup, and A is a union of right $H(A)$ -cosets; moreover, $H(A) \leq G$ is the unique maximal subgroup H for which A is a union of right H -cosets. Of course, if G is abelian, then we do not need to differentiate between left and right stabilizers and simply speak of the stabilizer of A , and when G is written additively, we have $H(A) = \{g \in G : g + A = A\}$. For $n \geq 1$, we let C_n denote a cyclic group of order n .

Given a normal subgroup $H \triangleleft G$, we let

$$\phi_H : G \rightarrow G/H$$

denote the canonical homomorphism. The index of a subgroup $H \leq G$ is denoted $|G : H|$. When G is finite, $|G : H| = |G|/|H|$. We use standard notation for the following important subgroups:

$$\begin{aligned} Z(G) &= \{g \in G : gx = xg \text{ for all } x \in G\} \triangleleft G \quad \text{is the } \textit{center} \text{ of } G, \\ [x, y] &= x^{-1}y^{-1}xy \in G \quad \text{is the } \textit{commutator} \text{ of the elements } x, y \in G, \\ G' &= [G, G] = \langle [x, y] : x, y \in G \rangle \triangleleft G \quad \text{is the } \textit{commutator subgroup} \text{ of } G, \quad \text{and} \\ C_G(A) &= C_G(\langle A \rangle) = \{g \in G : ga = ag \text{ for all } a \in A\} \leq G \quad \text{is the } \textit{centralizer} \text{ of } A \subset G. \end{aligned}$$

For a set P , we denote by $\mathcal{F}(P)$ the *free abelian monoid* with basis P . Then every $a \in \mathcal{F}(P)$ has a unique representation in the form

$$a = p_1 \cdot \dots \cdot p_\ell = \prod_{p \in P} p^{\mathbf{v}_p(a)}, \quad \text{where } p_1, \dots, p_\ell \in P, \quad \mathbf{v}_p(a) \in \mathbb{N}_0 \quad \text{and} \quad \mathbf{v}_p(a) = 0 \quad \text{for almost all } p \in P,$$

and we use all notation from elementary divisibility theory. In particular, $\mathbf{v}_p(a)$ is the *p-adic valuation* of a , $\text{supp}(a) = \{p \in P : \mathbf{v}_p(a) > 0\} \subset P$ is the *support* of a , $|a| = \ell = \sum_{p \in P} \mathbf{v}_p(a)$ is the *length* of a , and $\mathbf{h}(a) = \max\{\mathbf{v}_p(a) : p \in P\}$.

Sequences Over Groups. These are our main objects of study. As it is traditional in Combinatorial Number Theory, by a *sequence* over a group G we mean a finite, unordered sequence where the repetition of elements is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ (this point of view provides many technical advantages and was pushed forward by applications of Zero-Sum Theory in more algebraic fields, such as Multiplicative Ideal Theory and Factorization Theory; see the monographs [14, 17] or the surveys [13, 19, 28, 1]). So we freely use all notation from free abelian monoids for sequences, though for reason explained in the next paragraph, we denote multiplication in $\mathcal{F}(G)$ by the boldsymbol \cdot rather than by juxtaposition and use brackets for all exponentiation in $\mathcal{F}(G)$. In particular, a sequence $S \in \mathcal{F}(G)$ has the form

$$S = g_1 \cdot \dots \cdot g_\ell = \bullet_{i \in [1, \ell]} g_i \in \mathcal{F}(G) \quad (1)$$

with the $g_i \in G$ the terms of S . The identity $1_{\mathcal{F}(G)} \in \mathcal{F}(G)$ is called the *empty* or *trivial* sequence, which is simply the sequence having no terms. For $g \in G$,

$$\mathbf{v}_g(S) = |\{i \in [1, \ell] : g_i = g\}| \quad \text{denotes the } \textit{multiplicity} \text{ of } g \text{ in } S,$$

$$\mathbf{h}(S) = \max\{\mathbf{v}_g(S) : g \in G\} \quad \text{denotes the } \textit{maximum multiplicity} \text{ of a term of } S,$$

and $T \mid S$ denotes that T is a *subsequence* of S . Of course, for $T \in \mathcal{F}(G)$, we have $T \mid S$ if and only if $\mathbf{v}_g(T) \leq \mathbf{v}_g(S)$ for all $g \in G$, and in such case, $T^{[-1]} \cdot S$ or $S \cdot T^{[-1]}$ denotes the subsequence of S obtained by removing the terms of T from S , i.e., $\mathbf{v}_g(T^{[-1]} \cdot S) = \mathbf{v}_g(S) - \mathbf{v}_g(T)$ for all $g \in G$.

In order to distinguish between the group operation in G and the sequence operation in $\mathcal{F}(G)$, we use the boldsymbol \cdot for the operation in $\mathcal{F}(G)$, so $\mathcal{F}(G) = (\mathcal{F}(G), \cdot)$ (which coincides with the convention in the monographs [14, 17]) and only denote multiplication in G by juxtaposition of elements. In particular, if $S_1, S_2 \in \mathcal{F}(G)$ and $g_1, g_2 \in G$, then $S_1 \cdot S_2 \in \mathcal{F}(G)$ has length $|S_1| + |S_2|$, $S_1 \cdot g_1 \in \mathcal{F}(G)$ has length $|S_1| + 1$, $g_1 g_2 \in G$ is an element of G , but $g_1 \cdot g_2 \in \mathcal{F}(G)$ is a sequence of length 2. In order to avoid confusion between exponentiation of the group operation in G and exponentiation of the sequence operation \cdot in $\mathcal{F}(G)$, we use brackets to denote exponentiation in $\mathcal{F}(G)$:

$$g^{[k]} = \underbrace{g \cdot \dots \cdot g}_k \in \mathcal{F}(G) \quad \text{and} \quad T^{[k]} = \underbrace{T \cdot \dots \cdot T}_k \in \mathcal{F}(G),$$

for $g \in G$, $T \in \mathcal{F}(G)$ and $k \in \mathbb{N}_0$. When $T^{[k]} \mid S$, we extend exponentiation to include negative exponents by setting $S \cdot T^{[-k]} = S \cdot (T^{[k]})^{[-1]} \in \mathcal{F}(G)$. In particular, if $S \in \mathcal{F}(G)$, $g \in G$ and $k \in \mathbb{Z}$ with $k \geq -\mathbf{v}_g(S)$, then $S \cdot g^{[k]} \in \mathcal{F}(G)$ has length $|S| + k$.

Let $S \in \mathcal{F}(G)$ be a sequence notated as in (1). When G is written multiplicatively, we use

$$\pi(S) = \{g_{\tau(1)} \dots g_{\tau(\ell)} \in G : \tau \text{ a permutation of } [1, \ell]\} \subset G$$

to denote the *set of products* of S . In view of the basic properties of the commutator subgroup $G' = [G, G] \leq G$, it is readily seen that

$$\pi(S) \quad \text{is contained in a } G'\text{-coset.}$$

Note that $|S| = 0$ if and only if S is trivial, and in this case we use the convention that $\pi(S) = \{1\}$. When G is written additively with commutative operation, we likewise let

$$\sigma(S) = g_1 + \dots + g_\ell \in G$$

denote the *sum* of S . More generally, for any integer $n \geq 0$, the n -*sums* and n -*products* of S are respectfully denoted by

$$\Sigma_n(S) = \{\sigma(T) : T \mid S \text{ and } |T| = n\} \subset G \quad \text{and} \quad \Pi_n(S) = \bigcup_{\substack{T \mid S \\ |T|=n}} \pi(T) \subset G,$$

and the *subsequence sums* and *subsequence products* of S are respectively denoted by

$$\Sigma(S) = \bigcup_{n \geq 1} \Sigma_n(S) \subset G \quad \text{and} \quad \Pi(S) = \bigcup_{n \geq 1} \Pi_n(S) \subset G.$$

The sequence S is called

- a *product-one sequence* if $1 \in \pi(S)$,
- *product-one free* if $1 \notin \pi(S)$.

Zero-sum and zero-sum free sequences are analogously defined when G is written additively using σ in place of π and 0 in place of 1. Every map of groups $\varphi: G \rightarrow H$ extends to a monoid homomorphism $\varphi: \mathcal{F}(G) \rightarrow \mathcal{F}(H)$ by setting

$$\varphi(S) = \varphi(g_1) \cdot \dots \cdot \varphi(g_\ell) \in \mathcal{F}(H).$$

If φ is a group homomorphism, then $\varphi(S)$ is a product-one sequence if and only if $\pi(S) \cap \text{Ker}(\varphi) \neq \emptyset$.

We use

$$\mathcal{B}(G) = \{S \in \mathcal{F}(G) : 1 \in \pi(S)\}$$

to denote the set of all product-one sequences. Clearly, $\mathcal{B}(G) \subset \mathcal{F}(G)$ is a submonoid, hence a commutative, cancellative semigroup with unit element, and we denote by $\mathcal{A}(G) = \mathcal{A}(\mathcal{B}(G))$ the set of atoms (irreducible elements) of $\mathcal{B}(G)$. In other words, $\mathcal{A}(G)$ consists of the minimal product-one sequences, which are the nontrivial, product-one sequences that cannot be factored into two nontrivial, product-one subsequences. We call

$$D(G) = \sup\{|S| : S \in \mathcal{A}(G)\} \in \mathbb{N} \cup \{\infty\}$$

the *large Davenport constant* of G and

$$d(G) = \sup\{|S| : S \in \mathcal{F}(G) \text{ is product-one free}\} \in \mathbb{N}_0 \cup \{\infty\}$$

the *small Davenport constant* of G .

Suppose that G is abelian. Then $\mathcal{B}(G)$ is a Krull monoid (for more on Krull monoids, see [18, 7, 8]). More precisely (apart from the trivial case $|G| = 2$), the monoid $\mathcal{B}(G)$ is (up to isomorphism) the unique reduced Krull monoid with class group G in which every class contains exactly one prime divisor. When studying the arithmetic of general Krull monoids H (e.g., of integrally closed, noetherian domains) with class group G , many questions can be reduced to the associated monoid $\mathcal{B}(G)$ of zero-sum sequences over the class group [14, Section 3.4]. For instance, the large Davenport constant $D(G)$ is the supremum over all k for which there exists an atom $u \in H$ which is a product of k prime divisors [14, Theorem 5.1.5]. For rings of integers in algebraic number fields (which are Krull monoids), this was first observed by Rogers in 1963 [27]. Thus, from the very beginning up to the latest applications, it has always been the large Davenport constant which has been at the center of interest. In the abelian case, a simple argument (see Lemma 2.4) shows that $d(G) + 1 = D(G)$. Thus the small Davenport constant is a sufficient tool to study the large Davenport constant for abelian groups. For general groups, we only have the inequality $d(G) + 1 \leq D(G)$, and hence the study of the large Davenport constant requires additional efforts.

Ordered Sequences Over Groups. These are an important tool used to study (unordered) sequences over non-abelian groups. Indeed, it is quite useful to have related notation for sequences in which the order of terms matters. Thus we let $\mathcal{F}^*(G) = (\mathcal{F}^*(G), \cdot)$ denote the free (non-abelian) monoid with basis G , whose elements will be called the *ordered sequences* over G . In other terminology, $\mathcal{F}^*(G)$ is the semigroup of words on the alphabet G , and the elements are called words or strings.

Taking an ordered sequence in $\mathcal{F}^*(G)$ and considering all possible permutations of its terms gives rise to a natural equivalence class in $\mathcal{F}^*(G)$, yielding a natural map

$$[\cdot] : \mathcal{F}^*(G) \rightarrow \mathcal{F}(G)$$

given by abelianizing the sequence product in $\mathcal{F}^*(G)$. An ordered sequence $S^* \in \mathcal{F}^*(G)$ with $[S^*] = S$ is called an *ordering* of the sequence $S \in \mathcal{F}(G)$.

All notation and conventions for sequences extend naturally to ordered sequences. In particular, every map of groups $\varphi: G \rightarrow H$ extends uniquely to a monoid homomorphism $\varphi: \mathcal{F}^*(G) \rightarrow \mathcal{F}^*(H)$ and, for an ordered sequence $S^* \in \mathcal{F}^*(G)$ with $S = [S^*]$, we set $\mathbf{h}(S^*) = \mathbf{h}(S)$, $\text{supp}(S^*) = \text{supp}(S)$, $|S^*| = |S|$, and $\mathbf{v}_g(S^*) = \mathbf{v}_g(S)$ for every $g \in G$. Let

$$S^* = g_1 \cdot \dots \cdot g_\ell \in \mathcal{F}^*(G)$$

be an ordered sequence. For every subset $I \subset [1, \ell]$, we set

$$S^*(I) = \bullet_{i \in I} g_i \in \mathcal{F}^*(G), \tag{2}$$

where the product is taken in the natural order given by $I \subset \mathbb{Z}$, and every sequence of such a form in $\mathcal{F}^*(G)$ is called an (*ordered*) *subsequence* of S^* . We use the abbreviation

$$S^*(x, y) = S^*([x, y])$$

for integers $x, y \in \mathbb{Z}$. If $I = \emptyset$, then $S^*(I) = 1_{\mathcal{F}^*(G)}$ is the identity of $\mathcal{F}^*(G)$ (in other words, the empty ordered sequence), and if $T^* = S^*(I)$ with $I \subset [1, \ell]$ an interval, then we say that $T^* \in \mathcal{F}^*(G)$ is a subsequence of *consecutive terms*, or simply a *consecutive subsequence*, and we indicate this by writing $T^* \mid S^*$. If $i \in [1, |S^*|]$, then

$$S^*(i) = S^*([i, i]) \in G \quad \text{denotes the } i\text{-th term of } S^*.$$

Let $\pi: \mathcal{F}^*(G) \rightarrow G$ denote the unique homomorphism that maps an ordered sequence onto its product in G , so

$$\pi(S^*) = \prod_{i=1}^{\ell} g_i \in G.$$

If $\pi(S^*) = 1$, then S^* is called a *product-one ordered sequence*.

By a *factorization* of $S^* \in \mathcal{F}^*(G)$ of length r , we mean an r -tuple (S_1^*, \dots, S_r^*) of nontrivial, consecutive subsequences $S_i^* \mid S^*$ such that $S^* = S_1^* \cdot \dots \cdot S_r^*$. Informally speaking, we may refer to $S^* = S_1^* \cdot \dots \cdot S_r^*$ as a factorization of S^* as well. Then, for each $i \in [1, r]$, we have $S_i^* = S^*(I_i)$ for some $I_i \subset [1, |S|]$ such that

$$\bigcup_{i=1}^r I_i = [1, |S|] \quad \text{and} \quad \max I_j = \min I_{j+1} - 1 \quad \text{for } j \in [1, r-1].$$

Given such a factorization of S^* , we can define a new ordered sequence

$$T^* = \pi(S_1^*) \cdot \dots \cdot \pi(S_r^*) \in \mathcal{F}^*(G),$$

so T^* is obtained from S^* by replacing consecutive subsequences with the product of their terms. It is then readily noted that

$$\pi(T^*) = \pi(S^*) \quad \text{and} \quad \pi([T^*]) \subset \pi([S^*]).$$

Moreover, if $[S^*] \in \mathcal{A}(G)$ was an atom, then $[T^*] \in \mathcal{A}(G)$ must remain an atom.

Basic Lemmas Regarding Sequences. We now prove several basic lemmas and observations that will be needed repeatedly in the paper. The first two are rather straightforward but frequently needed.

Lemma 2.1. *Let G be a group and let $U^* \in \mathcal{F}^*(G)$ be an ordered sequence with $\pi(U^*) = 1$ and $[U^*] \in \mathcal{A}(G)$ an atom. Then there are no consecutive, product-one subsequences of U^* that are proper and nontrivial.*

Proof. Observe that removing a consecutive, product-one subsequence from an ordered sequence does not affect its product. Thus, if the product-one ordered sequence U^* had a consecutive, product-one subsequence that was proper and nontrivial, say $U^*(I)$ with $I \subset [1, |U^*|]$ an interval, then $[U^*] = [U^*(I)] \cdot [U^*([1, |U^*|] \setminus I)]$ would be a factorization of $[U^*]$ into two nontrivial, product-one subsequences, contradicting that $[U^*] \in \mathcal{A}(G)$ is an atom. \square

Lemma 2.2. *Let G be group with $G' = [G, G] \leq G$ its commutator subgroup, and let $S \in \mathcal{F}(G)$ be a product-one sequence. If $T \mid S$ is a subsequence with $\pi(T) \subset G'$, then $\pi(T^{[-1]} \cdot S) \subset G'$. In particular, if $T \mid S$ is a product-one subsequence, then $\pi(T^{[-1]} \cdot S) \subset G'$.*

Proof. As remarked earlier in the section, we know that every sequence $R \in \mathcal{F}(G)$ has $\pi(R)$ contained in a G' -coset. In other words, $\phi_{G'}(\pi(R))$ is a single-element, and any product-one sequence R has $1 \in \pi(R) \subset G'$. Thus $\pi(S) \subset G'$ and $\pi(T) \subset G'$ follow from our hypotheses and, consequently,

$$\phi_{G'}(\pi(T^{[-1]} \cdot S)) = \phi_{G'}(\pi(T))^{-1} \phi_{G'}(\pi(S)) = \{1\}^{-1} \{1\} = \{1\},$$

which means $\pi(T^{[-1]} \cdot S) \subset G'$, as desired. \square

The next lemma shows that a product-one ordered sequence can have its terms cyclically shifted while preserving its product.

Lemma 2.3. *Let G be a group and let $S = g_1 \cdot \dots \cdot g_\ell \in \mathcal{F}^*(G)$ be a product-one ordered sequence. Then $g_j \cdot \dots \cdot g_\ell \cdot g_1 \cdot \dots \cdot g_{j-1}$ is also a product-one ordered sequence for every $j \in [1, \ell]$.*

Proof. Let $S' = g_\ell \cdot g_1 \cdot \dots \cdot g_{\ell-1} \in \mathcal{F}^*(G)$. Since S has product-one, we have

$$\pi(S') = g_\ell g_1 \dots g_{\ell-1} = g_\ell (g_1 \dots g_\ell) g_\ell^{-1} = g_\ell \pi(S) g_\ell^{-1} = g_\ell 1 g_\ell^{-1} = 1.$$

Therefore S' is also a product-one ordered sequence. Iterating this argument $\ell - j + 1$ times shows that $g_j \cdot \dots \cdot g_\ell \cdot g_1 \cdot \dots \cdot g_{j-1}$ is a product-one ordered sequence, as desired. \square

The next lemma is proved by a standard argument. In particular, the statements for abelian groups are well-known. We provide the full proof so that the reader may become acquainted with the notation.

Lemma 2.4. *Let G be a group.*

1. If G is finite, then every ordered sequence $S \in \mathcal{F}^*(G)$ of length $|S| \geq |G|$ has a consecutive, product-one subsequence that is nontrivial. In particular, we have $\mathbf{d}(G) + 1 \leq \mathbf{D}(G) \leq |G|$.
2. G is finite if and only if $\mathbf{d}(G)$ is finite.
3. If G is finite abelian, then $\mathbf{d}(G) + 1 = \mathbf{D}(G)$.
4. If G is finite cyclic, then $\mathbf{d}(G) + 1 = \mathbf{D}(G) = |G|$.

Proof. 1. Let $S \in \mathcal{F}^*(G)$ be an ordered sequence of length $|S| = \ell \geq |G|$. For $j \in [1, \ell]$, we consider the elements $\pi(S(1, j)) \in G$. If $\pi(S(1, j)) = 1$ for some $j \in [1, \ell]$, then $S(1, j)$ is the desired consecutive, product-one subsequence. Otherwise, $\ell = |S| \geq |G|$ together with the pigeonhole principle guarantees that there are $j, k \in [1, \ell]$ with $j < k$ and $\pi(S(1, j)) = \pi(S(1, k))$, and then $S(j+1, k)$ is the desired consecutive, product-one subsequence.

It is now clear from Lemma 2.1 that $\mathbf{D}(G) \leq |G|$. If $S \in \mathcal{F}(G)$ is product-one free and $g \in \pi(S)$, then $S \cdot g^{-1} \in \mathcal{A}(G)$, and hence $\mathbf{d}(G) + 1 \leq \mathbf{D}(G)$.

2. By Item 1, it suffices to show that $\mathbf{d}(G) = \infty$ when $|G| = \infty$. Suppose that G is infinite and let $S \in \mathcal{F}(G)$ be product-one free. If we can show that there is a product-one free sequence of length $|S| + 1$, then the assertion follows. Since G is infinite but $|\pi(S)| \leq 2^{|S|} < \infty$, there is an element $g^{-1} \in G \setminus \Pi(S)$, and we assert that $S \cdot g^{-1}$ is product-one free. Assume to the contrary that $1 \in \Pi(S \cdot g^{-1})$. Then, since S is product-one free, there must exist a product-one subsequence $T \mid S \cdot g^{-1}$ with $g^{-1} \in \text{supp}(T)$. Let $T^* = g_1 \cdot \dots \cdot g_{|T|} \in \mathcal{F}^*(G)$ be an ordering of T such that $\pi(T^*) = 1$. Then, by Lemma 2.3, we can w.l.o.g. assume $T^*(1) = g^{-1}$, i.e., that $g_1 = g^{-1}$, whence $g = g_1^{-1} = g_2 \cdot \dots \cdot g_{|T|} \in \pi(T \cdot (g^{-1})^{[-1]}) \subset \Pi(S)$, contradicting that $g \in G \setminus \Pi(S)$. So $S \cdot g^{-1}$ is product-one free as claimed, completing the proof of Item 2.

3. Let $U \in \mathcal{A}(G)$ be an atom with $|U| = \mathbf{D}(G)$ and let $g \in \text{supp}(G)$. Now consider $S = U \cdot g^{[-1]}$. Then $|S| = |U| - 1 = \mathbf{D}(G) - 1$, and it suffices in view of Item 1 to show that S is product-one free. Assuming this fails, then there must be a nontrivial, product-one subsequence $T \mid S$. Since $S \mid U$ is a proper subsequence, this ensures that $T \mid U$ is a proper, nontrivial, product-one subsequence of U . However, since G is abelian with T and U both product-one sequences, we have $\pi(T^{[-1]} \cdot U) = \pi(T)\pi(T^{[-1]} \cdot U) = \pi(U) = 1$, so that $U = T \cdot (T^{[-1]} \cdot U)$ is a factorization of U into two nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. Thus S is product-one free, completing the proof of Item 3 as noted above.

4. If $g \in G$ with $\text{ord}(g) = |G|$, then the sequence $S = g^{[|G|-1]} \in \mathcal{F}(G)$ is product-one free, hence $|G| - 1 \leq \mathbf{d}(G)$, and thus the assertion follows from Item 1. \square

We are not aware of a finite, non-abelian group with $\mathbf{d}(G) + 1 = \mathbf{D}(G)$ (see also Lemma 3.4). Next we give a characterization for the large Davenport constant.

Lemma 2.5. *Let G be a finite group. Then $\mathbf{D}(G)$ is the smallest integer $\ell \in \mathbb{N}$ with the following property: for every sequence $S \in \mathcal{F}(G)$ of length $|S| \geq \ell$ and every $x \in \pi(S)$, there exists a nontrivial, product-one subsequence $T \mid S$ with $x \in \pi(T^{[-1]} \cdot S)$ and $|T| \leq \ell$.*

Proof. First we show that $\mathbf{D}(G)$ has the required property. Suppose $S \in \mathcal{F}(G)$ with $|S| \geq \mathbf{D}(G)$ and let $x \in \pi(S)$. Then $S \cdot x^{-1} \in \mathcal{F}(G)$ is a product-one sequence with length $|S \cdot x^{-1}| = |S| + 1 > \mathbf{D}(G)$. Repeatedly applying the definition of $\mathbf{D}(G)$ to the product-one sequence $S \cdot x^{-1}$ results in a factorization $S \cdot x^{-1} = T_1 \cdot \dots \cdot T_r$ with $T_i \in \mathcal{A}(G)$ atoms having

$$1 \leq |T_i| \leq \mathbf{D}(G) \quad \text{for } i \in [1, r]. \quad (3)$$

Since $|S \cdot x^{-1}| > D(G)$, it follows that $r \geq 2$. Without restriction, we may assume $x^{-1} \in \text{supp}(T_1)$, and then it is clear that $T_2 \cdot \dots \cdot T_r \mid S$ is a nontrivial, product-one subsequence (in view of $r \geq 2$) with

$$(T_2 \cdot \dots \cdot T_r)^{[-1]} \cdot S = T_1 \cdot (x^{-1})^{[-1]}. \quad (4)$$

Since T_1 is a product-one sequence, there is an ordering of the terms of T_1 having product 1, say $T_1 = x_1 \cdot \dots \cdot x_n$ with $x_1 \dots x_n = 1$. In view of Lemma 2.3, we can cyclically shift the ordering so that $x^{-1} \in \text{supp}(T_1)$ is the first term while preserving that the product of terms is 1, i.e., we may w.l.o.g. assume $x_1 = x^{-1}$. But now it is clear using (4) that

$$x = x_1^{-1} = x_2 \dots x_{n-1} \in \pi(T_1 \cdot x_1^{[-1]}) = \pi(T_1 \cdot (x^{-1})^{[-1]}) = \pi((T_2 \cdot \dots \cdot T_r)^{[-1]} \cdot S) \subset \pi(T_2^{[-1]} \cdot S).$$

Thus, in view of (3), it follows that $T = T_2$ is the desired product-one subsequence of S .

To show that $D(G)$ is the smallest integer with the desired property, consider an atom $U \in \mathcal{A}(G)$ with $|U| = D(G)$ and an element $x^{-1} \in \text{supp}(U)$, say $U = S \cdot x^{-1}$ where $S \in \mathcal{F}(G)$ with $|S| = D(G) - 1$. Moreover, as argued above using Lemma 2.3, we have $x \in \pi(S)$. If by contradiction S contained a nontrivial, product-one subsequence $T \mid S$ with $x \in \pi(T^{[-1]} \cdot S)$, then $U = T \cdot (T^{[-1]} \cdot S \cdot x^{-1}) = T \cdot (T^{[-1]} \cdot U)$ would be a factorization of U into nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. \square

Finally, we need the concept of a *setpartition*. Let P be a set and let Q be the set of *finite and nonempty* subsets of P . The elements of $\mathcal{S}(P) := \mathcal{F}(Q)$ are called *setpartitions over P* , and an *n -setpartition*, where $n \geq 0$, is simply a setpartition $\mathcal{A} \in \mathcal{S}(P)$ having length $|\mathcal{A}| = n$. In other words, an n -setpartition $\mathcal{A} = A_1 \cdot \dots \cdot A_n \in \mathcal{S}(P)$ is a sequence of n finite and *nonempty* subsets $A_i \subset P$. The setpartition $\mathcal{A} \in \mathcal{S}(P)$ naturally partitions the sequence

$$S(\mathcal{A}) = \underset{i \in [1, n]}{\bullet} \underset{a \in A_i}{\bullet} a \in \mathcal{F}(P),$$

and \mathcal{A} is said to have its terms being of *as near equal a size as possible* if

$$|A_i| \in \left\{ \left\lfloor \frac{|S(\mathcal{A})|}{n} \right\rfloor, \left\lceil \frac{|S(\mathcal{A})|}{n} \right\rceil \right\} \quad \text{for all } i \in [1, n].$$

A sequence $S \in \mathcal{F}(P)$ is said to *have an n -setpartition* if there is an n -setpartition $\mathcal{A} \in \mathcal{S}(P)$ with $S(\mathcal{A}) = S$. The following is the standard existence result for setpartitions. It can be found in [17, Proposition 10.2] or [4].

Lemma 2.6. *Let P be a set, let $S \in \mathcal{F}(P)$ be a sequence over P , and let $\ell \geq 0$ and $n \geq 1$ be integers. Then there is a subsequence $S' \mid S$ with $|S'| = \ell + n$ having an n -setpartition if and only if*

$$|S| \geq \ell + n \quad \text{and,} \quad \text{for every nonempty subset } X \subset P \text{ with } |X| \leq \frac{\ell-1}{n} + 1, \\ \text{there are at most } |S| - \ell + (|X| - 1)n \text{ terms of } S \text{ from } X.$$

Moreover, if this is the case, then S' has an n -setpartition with terms of as near equal a size as possible.

In particular, S has an n -setpartition if and only if $h(S) \leq n \leq |S|$, and if this is the case, then S has an n -setpartition with terms of as near equal a size as possible.

3. GENERAL UPPER BOUNDS

We begin with the following upper bound of Olson and White [26] for the small Davenport constant.

Theorem 3.1. *Let G be a finite, noncyclic group. Then*

$$d(G) \leq \frac{1}{2}|G|$$

with equality if G contains a cyclic, index 2 subgroup.

The following gives an inductive upper bound for the large Davenport constant. We are indebted to an anonymous referee for having suggested the key idea at the heart of its proof.

Theorem 3.2. *Let G be a finite group and let $H \leq G$ be a subgroup. Then*

$$D(G) \leq D(H)|G : H|.$$

Proof. The proof is similar to that of Lemma 2.4. We need to show that $|U| \leq D(H)|G : H|$ for all $U \in \mathcal{A}(G)$. Assume by contradiction that there is some $U \in \mathcal{A}(G)$ with $|U| > D(H)|G : H|$. Since $U \in \mathcal{A}(G)$, there exists a product-one ordered sequence $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$.

For every $j \in [1, |U|]$, we consider the elements $\pi(U^*(1, j)) \in G$. Since $|U| > D(H)|G : H|$, the pigeonhole principle guarantees that there exists some left H -coset, say gH , for which $\pi(U^*(1, j)) \in gH$ holds for at least $D(H) + 1$ values of $j \in [1, |U|]$. Let $j_1 < j_2 < \dots < j_r$, where $r \geq D(H) + 1$, be all those indices $j_i \in [1, |U|]$ with $\pi(U^*(1, j_i)) \in gH$. Our next goal is to show that, by cyclically shifting the ordered sequence U^* , we can w.l.o.g. assume $j_r = |U|$.

Consider the ordered sequence $U'^* = U^*(j_r + 1, |U|) \cdot U^*(1, j_r) \in \mathcal{F}^*(G)$. Clearly, we have $[U'^*] = [U^*] = U$. However, we also have

$$\begin{aligned} \pi(U'^*) &= \pi(U^*(j_r + 1, |U|))\pi(U^*(1, j_r)) = \pi(U^*(j_r + 1, |U|))\pi(U^*)\pi(U^*(j_r + 1, |U|))^{-1} \\ &= \pi(U^*(j_r + 1, |U|))1\pi(U^*(j_r + 1, |U|))^{-1} = 1. \end{aligned}$$

Thus U'^* is a product-one ordered sequence with $[U'^*] = U$. Moreover, letting $s = |U^*(j_r + 1, |U^*|)| = |U^*| - j_r$ and $g' = \pi(U^*(j_r + 1, |U^*|))$, we see (in view of the definition of the j_i) that

$$\pi(U'^*(1, j_i + s)) = g'\pi(U(1, j_i)) \in g'gH \quad \text{for all } i \in [1, r].$$

Consequently, repeating the above arguments using the ordered sequence U'^* in place of U^* allows us to w.l.o.g. assume $j_r = |U^*|$. But then $1 = \pi(U^*) = \pi(U^*(1, |U^*|)) = \pi(U^*(1, j_r)) \in gH$ forces $gH = H$. Thus we now have

$$\pi(U^*(1, j_i)) \in H \quad \text{for } i \in [1, r]. \tag{5}$$

Let $U_i^* = U^*(j_{i-1} + 1, j_i) \in \mathcal{F}^*(G)$ for $i \in [1, r]$, where $j_0 := 0$. Since $j_r = |U|$, we have

$$U_1^* \cdot \dots \cdot U_r^* = U^*. \tag{6}$$

In view of (5), we have

$$\pi(U_1^*), \pi(U_1^* \cdot U_2^*), \pi(U_1^* \cdot U_2^* \cdot U_3^*), \dots, \pi(U_1^* \cdot \dots \cdot U_r^*) \in H.$$

A simple inductive argument now shows

$$\pi(U_i^*) \in H \quad \text{for all } i \in [1, r]. \quad (7)$$

In view of (6) and (7), consider the sequence $S = \pi(U_1^*) \cdot \dots \cdot \pi(U_r^*) \in \mathcal{F}(H)$. Since $\pi(U_1^*) \dots \pi(U_r^*) = \pi(U_1^* \dots U_r^*) = \pi(U^*) = 1$, we see that $S \in \mathcal{B}(H)$. However, since $|S| = r \geq D(H) + 1$, the definition of $D(H)$ ensures that we have some factorization of S , say

$$S = \left(\bullet_{i \in I} \pi(U_i^*) \right) \left(\bullet_{i \in [1, r] \setminus I} \pi(U_i^*) \right),$$

where $I \subset [1, r]$, with both $\bullet_{i \in I} \pi(U_i^*)$ and $\bullet_{i \in [1, r] \setminus I} \pi(U_i^*)$ nontrivial, product-one sequences over $H \leq G$.

But then it is clear that both $\left[\bullet_{i \in I} U_i^* \right]$ and $\left[\bullet_{i \in [1, r] \setminus I} U_i^* \right]$ are nontrivial, product-one sequences over G , whence the factorization (in view of (6))

$$U = [U^*] = \left[\bullet_{i \in I} U_i^* \right] \cdot \left[\bullet_{i \in [1, r] \setminus I} U_i^* \right]$$

contradicts that $U \in \mathcal{A}(G)$ is an atom, completing the proof. \square

A similar argument to that of Theorem 3.2 gives the following result.

Theorem 3.3. *Let G be a finite group and let $H \triangleleft G$ be a normal subgroup with $H \cap G' = \{1\}$, where $G' = [G, G] \leq G$ is the commutator subgroup of G . Then*

$$D(G) \leq D(H)D(G/H).$$

Proof. Assume by contradiction that there is some atom $U \in \mathcal{A}(G)$ with $|U| > D(H)D(G/H)$. Since U is a product-one sequence, we have $1 \in \pi(U) \subset G'$. Since $|U| > D(H)D(G/H)$, repeatedly applying Lemma 2.5 to the product-one sequence $\phi_H(U) \in \mathcal{F}(G/H)$ taking $x = 1$ each time yields a factorization

$$U = U_1 \cdot \dots \cdot U_r \quad \text{with} \quad \pi(U_i) \cap H \neq \emptyset \quad \text{for } i \in [1, r] \quad \text{and} \quad r > D(H).$$

Since $\pi(U_i) \cap H \neq \emptyset$ for $i \in [1, r]$, it follows that each $U_i \in \mathcal{F}(G)$ has an ordering $U_i^* \in \mathcal{F}^*(G)$, so $[U_i^*] = U_i$, such that $\pi(U_i^*) \in H$. As a result, $\pi(U_1^*) \dots \pi(U_r^*) \in H$. However, we also have

$$\pi(U_1^*) \dots \pi(U_r^*) \in \pi([U_1^* \dots U_r^*]) = \pi(U) \subset G'.$$

Thus, in view of the hypothesis $H \cap G' = \{1\}$, it follows that $\pi(U_1^*) \dots \pi(U_r^*) = 1$. But this shows that

$$U' := \pi(U_1^*) \cdot \dots \cdot \pi(U_r^*) \in \mathcal{F}(H)$$

is a product-one sequence of length $r > D(H)$. Consequently, the definition of $D(H)$ ensures that there is a factorization

$$U' = \left(\bullet_{i \in I} \pi(U_i^*) \right) \cdot \left(\bullet_{i \in [1, r] \setminus I} \pi(U_i^*) \right)$$

with $\left(\bullet_{i \in I} \pi(U_i^*) \right)$ and $\left(\bullet_{i \in [1, r] \setminus I} \pi(U_i^*) \right)$ both nontrivial, product-one subsequences of U' , where $I \subset [1, r]$.

But then $U = \left[\bullet_{i \in I} U_i^* \right] \cdot \left[\bullet_{i \in [1, r] \setminus I} U_i^* \right]$ is a factorization of U into 2 nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. \square

Next, we give an upper bound in the case when G is nearly abelian.

Lemma 3.4. *Let G be a finite group with commutator subgroup $G' = [G, G] \leq G$. Suppose $|G'| \leq 2$. Then*

$$D(G) \leq d(G) + |G'|.$$

Proof. If $|G'| = 1$, then G is abelian and $d(G) + 1 = D(G)$ holds by Lemma 2.4. Therefore we may assume $|G'| = 2$. Assume by contradiction that we have an atom $U \in \mathcal{A}(G)$ with

$$|U| = D(G) \geq d(G) + |G'| + 1 = d(G) + 3. \quad (8)$$

If all the terms of U commute with each other, then $\text{supp}(U)$ generates an abelian group, whence

$$|U| \leq D(\langle \text{supp}(U) \rangle) = d(\langle \text{supp}(U) \rangle) + 1 \leq d(G) + 1,$$

contrary to (8). Therefore we may assume there are terms $x, y \in \text{supp}(U)$ which do not commute with each other: $xy \neq yx$. Let $T = x \cdot y \in \mathcal{F}(G)$ be the subsequence consisting of these 2 terms. Since the terms of T do not commute with each other, we have $|\pi(T)| = 2 = |G'|$, and since $\pi(T)$ must be contained in a G' -coset (as noted in Section 2), this ensures that $\pi(T)$ is an entire G' -coset. In view of (8), we have $|T^{[-1]} \cdot U| = |U| - 2 \geq d(G) + 1$. Thus the definition of $d(G)$ ensures that there is a nontrivial, product-one subsequence $R \mid T^{[-1]} \cdot U$. From Lemma 2.2, we know that $\pi(R^{[-1]} \cdot U) \subset G'$. Thus, since $|\pi(T)| = |G'|$ with $T \mid R^{[-1]} \cdot U$, we conclude that $\pi(R^{[-1]} \cdot U) = G'$. In particular, $1 \in \pi(R^{[-1]} \cdot U)$, meaning $R^{[-1]} \cdot U$ is also a product-one subsequence, which is nontrivial in view of $T \mid R^{[-1]} \cdot U$ and $|T| = 2$. But now $U = R \cdot (R^{[-1]} \cdot U)$ is a factorization of U into 2 nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. \square

4. SOME TOOLS FROM ADDITIVE THEORY

In this section, we present the results from Additive Theory needed for Theorem 1.1. To simplify notation, all groups in this section will be abelian and written additively. We begin with the classical Cauchy-Davenport Theorem [17, Theorem 6.2].

Theorem 4.1 (Cauchy-Davenport Theorem). *Let G be an abelian group of prime order p and let $A_1, \dots, A_n \subset G$ be nonempty subsets. Then*

$$|\sum_{i=1}^n A_i| \geq \min\{p, \sum_{i=1}^n |A_i| - n + 1\}.$$

Next, we state the following special case of either the DeVos-Goddyn-Mohar Theorem or the Partition Theorem (see [17, Chapters 13 and 14] or [6]).

Theorem 4.2. *Let G be an abelian group, let $S \in \mathcal{F}(G)$ be a sequence, let $n \in [1, |S|]$, and let $H = H(\Sigma_n(S))$. Then*

$$|\Sigma_n(S)| \geq \left(\sum_{g \in G/H} \min\{n, \nu_g(\phi_H(S))\} - n + 1 \right) |H|. \quad (9)$$

For the proof of Theorem 1.1, the case when G is isomorphic to the dicyclic group Q_{4p} of order $4p$ with $p \geq 3$ prime proves to be particularly difficult. One of the key ideas for handling this case is to reduce the basic product-one question for the non-abelian group Q_{4p} into a more complicated zero-sum question over the abelian group C_{2p} : Lemma 4.3. However, we first need some additional notation.

Given an additively written, abelian group G , we let

$$2G = \{2g : g \in G\} \leq G$$

denote the homomorphic image of G under the multiplication by 2 homomorphism. Likewise, given a sequence $S = g_1 \cdot \dots \cdot g_\ell \in \mathcal{F}(G)$, we let

$$2S = 2g_1 \cdot \dots \cdot 2g_\ell \in \mathcal{F}(2G).$$

For the following lemma, we will make use of the fact that

$$\bigcup_{T|S, |T|=n} \left(\sigma(T) - \sigma(S \cdot T^{[-1]}) \right) = \Sigma_n(2S) - \sigma(S) \quad (10)$$

for any sequence $S \in \mathcal{F}(G)$ with $|S| \geq n \geq 1$ —the equality follows routinely from the definitions involved.

We remark that Lemma 4.3 remains true without assuming $p \geq 2$ is prime. However, the proof is much more technical and requires a somewhat detailed case distinction for defining and dealing with the subsequence S' in the proof. As we only need the case when p is prime, we have opted to present the simplified proof. Moreover, we will actually show Lemma 4.3 holds with $|U_1| = |U_2| \leq 2$.

Lemma 4.3. *Let G be a cyclic group of order $|G| = 2p$ with $p \geq 2$ prime, let $x \in G$ be the unique element with $\text{ord}(x) = 2$, and let $S \in \mathcal{F}(G)$ be a sequence of even length $|S| \geq 2p + 4$. Suppose there is a factorization*

$$S = T_1 \cdot T_2 \quad \text{with} \quad |T_1| = |T_2| = \frac{1}{2}|S| \quad \text{and} \quad \sigma(T_1) - \sigma(T_2) = |T_1|x,$$

where $T_1, T_2 \in \mathcal{F}(G)$. Then there is a factorization $S = U_1 \cdot U_2 \cdot V_1 \cdot V_2$, where $U_1, U_2, V_1, V_2 \in \mathcal{F}(G)$ are nontrivial, such that

$$|U_1| = |U_2|, \quad |V_1| = |V_2|, \quad \sigma(U_1) - \sigma(U_2) = |U_1|x \quad \text{and} \quad \sigma(V_1) - \sigma(V_2) = |V_1|x. \quad (11)$$

Proof. Let $|S| = 2\ell \geq 2p + 4 \geq 8$, so that

$$|T_1| = |T_2| = \ell \geq p + 2 \geq 4. \quad (12)$$

Note $x = -x$ and

$$|T_1|x = \begin{cases} 0, & \text{if } |T_1| = \ell \text{ is even} \\ x, & \text{if } |T_1| = \ell \text{ is odd.} \end{cases}$$

If $g \in \text{supp}(T_1)$ with $g + x \in \text{supp}(T_2)$ for some $g \in G$, then the lemma follows setting $U_1 = g$, $U_2 = x + g$, $V_1 = T_1 \cdot g^{[-1]}$ and $V_2 = T_2 \cdot (x + g)^{[-1]}$ —in view of the hypotheses $|T_1| = |T_2| = \ell \geq 2$ and $\sigma(T_1) - \sigma(T_2) = |T_1|x$. Likewise, if there is some $g \in G$ with $\mathbf{v}_g(T_1), \mathbf{v}_g(T_2) \geq 2$, then the lemma follows setting $U_1 = U_2 = g^{[2]}$, $V_1 = T_1 \cdot g^{[-2]}$ and $V_2 = T_2 \cdot g^{[-2]}$ —in view of $|T_1| = |T_2| = \ell \geq 3$. Therefore, we may assume

$$(\text{supp}(T_1) + x) \cap \text{supp}(T_2) = \emptyset \quad \text{and} \quad (13)$$

$$\min\{\mathbf{v}_g(T_1), \mathbf{v}_g(T_2)\} \leq 1 \quad \text{for all } g \in G. \quad (14)$$

In particular,

$$\mathbf{h}(S) = \mathbf{h}(T_1 \cdot T_2) \leq \max\{|T_1| + 1, |T_2| + 1\} = \ell + 1. \quad (15)$$

Since $G \cong C_{2p}$, given any $\alpha \in G$, there are exactly 2 distinct elements $g, h \in G$ such that $2g = 2h = \alpha$.

Observing that it suffices to prove the lemma for any translated sequence $-g + S$, where $g \in G$ (the conclusions and hypotheses of the lemma are translation invariant), we may w.l.o.g. translate our sequence S so that

$$v_0(2S) = h(2S). \quad (16)$$

Note that

$$2S \in \mathcal{F}(2G) \quad \text{with} \quad 2G \cong C_p.$$

If $h(2S) \leq 2$, then (12) gives $2p + 4 \leq 2\ell = |S| = |2S| \leq h(2S)|2G| \leq 2p$, a contradiction. Therefore we have

$$v_0(2S) = h(2S) \geq 3. \quad (17)$$

By translating by $-x$ if need be, which preserves (16) since $2x = 0$, we may w.l.o.g. assume

$$v_0(S) \geq v_x(S). \quad (18)$$

We distinguish two cases.

Case 1: $x \in \text{supp}(S)$.

In view of $x \in \text{supp}(S)$ and (18), we have $0, x \in \text{supp}(S)$. Set $S' = S \cdot 0^{[-1]} \cdot x^{[-1]}$ and $\ell' = \frac{1}{2}|S'| = \ell - 1$. Since $0, x \in \text{supp}(S)$, it follows from (13) that either $\text{supp}(T_1) \cap \{0, x\} = \emptyset$ or $\text{supp}(T_2) \cap \{0, x\} = \emptyset$. Combining this with (16), we conclude that

$$h(2S) = v_0(2S) \leq \max\{|T_1|, |T_2|\} = \ell. \quad (19)$$

We will show that

$$\ell'x \in \bigcup_{T|S', |T|=\ell'} \left(\sigma(T) - \sigma(S' \cdot T^{[-1]}) \right) = \Sigma_{\ell'}(2S') - \sigma(S'), \quad (20)$$

where the equality above was noted in (10). Once (20) is established, we will know there exists some subsequence $T \mid S' = S \cdot 0^{[-1]} \cdot x^{[-1]}$ such that

$$\ell'x = |T| = 2\ell' - \ell' = |S'| - |T| = |S' \cdot T^{[-1]}| \quad \text{and} \quad \sigma(T) - \sigma(S' \cdot T^{[-1]}) = \ell'x = |T|x,$$

whence the lemma will follow setting $U_1 = 0$, $U_2 = x$, $V_1 = T$ and $V_2 = S' \cdot T^{[-1]}$. Thus it remains to establish (20) for the sequence S' to complete Case 1. For this, we apply Theorem 4.2 to $\Sigma_{\ell'}(2S')$.

In view of the hypotheses $S = T_1 \cdot T_2$ with $\sigma(T_1) - \sigma(T_2) = |T_1|x = \ell x$, we know

$$\sigma(S) = 2\sigma(T_2) + \ell x = 2\sigma(T_2) + \ell'x + x.$$

Thus

$$\sigma(S') + \ell'x = \sigma(S) - x + \ell'x = 2\sigma(T_2) + 2\ell'x = 2\sigma(T_2) \in 2G.$$

Consequently, if $\Sigma_{\ell'}(2S') = 2G$, then $2\sigma(T_2) = \sigma(S') + \ell'x \in \Sigma_{\ell'}(2S')$ follows, yielding (20), as desired. Therefore we may assume

$$|\Sigma_{\ell'}(2S')| \leq |2G| - 1 = p - 1. \quad (21)$$

Consequently, since $2G \cong C_p$ has no nontrivial, proper subgroups, we must have $H(\Sigma_{\ell'}(2S'))$ trivial. Since $H(\Sigma_{\ell'}(2S'))$ is trivial and $\ell' = \ell - 1 \geq p + 1$ (by (12)), Theorem 4.2 will contradict (21) if $2S'$ contains 2 distinct terms each having multiplicity at least $\ell' + 1$. Thus there can be at most one distinct term with multiplicity at least $\ell' + 1$ in $2S'$. Furthermore, Theorem 4.2 will again contradict (21) unless such a term from $2S'$ exists having multiplicity at least $2\ell' - p + 2 = 2\ell - p \geq \ell + 2$, where the inequality

follows from (12). However the latter contradicts (19) in view of the trivial inequality $h(2S') \leq h(2S)$, completing Case 1.

Case 2: $x \notin \text{supp}(S)$.

Since $x \notin \text{supp}(S)$, it follows from (17) that

$$v_0(S) = v_0(S) + v_x(S) = v_0(2S) \geq 3.$$

If $h(S \cdot 0^{[-2]}) \leq 1$, then it follows in view of the case hypothesis that

$$2p + 2 \leq |S| - 2 = |S \cdot 0^{[-2]}| \leq |G \setminus \{x\}| = 2p - 1,$$

a contradiction. Therefore we must instead have some $g \in \text{supp}(S \cdot 0^{[-2]})$ with $v_g(S \cdot 0^{[-2]}) \geq 2$, allowing us to define $S' := S \cdot 0^{[-2]} \cdot g^{[-2]}$. Let $\ell' = \ell - 2 = \frac{1}{2}|S'|$. Note that S' is nontrivial in view of $|S| = 2\ell \geq 2p + 4 \geq 8$. For the moment, $g \in \text{supp}(S \cdot 0^{[-2]})$ is an arbitrary element with $v_g(S \cdot 0^{[-2]}) \geq 2$. We will choose g more carefully later in the proof.

Next, we will show that

$$\ell'x \in \bigcup_{T|S', |T|=\ell'} \left(\sigma(T) - \sigma(S' \cdot T^{[-1]}) \right) = \Sigma_{\ell'}(2S') - \sigma(S'), \quad (22)$$

where the equality above was noted in (10). Once (22) is established, we will know there exists some subsequence $T \mid S' = S \cdot 0^{[-2]} \cdot g^{[-2]}$ such that

$$\ell'x = |T| = 2\ell' - \ell' = |S'| - |T| = |S' \cdot T^{[-1]}| \quad \text{and} \quad \sigma(T) - \sigma(S' \cdot T^{[-1]}) = \ell'x = |T|x,$$

whence the lemma will follow setting $U_1 = 0 \cdot g$, $U_2 = 0 \cdot g$, $V_1 = T$ and $V_2 = S' \cdot T^{[-1]}$. Thus it remains to establish (22) for the sequence S' to complete Case 2. For this, we apply Theorem 4.2 to $\Sigma_{\ell'}(2S')$.

In view of the hypotheses $S = T_1 \cdot T_2$ with $\sigma(T_1) - \sigma(T_2) = |T_1|x = \ell x$, we know

$$\sigma(S) = 2\sigma(T_2) + \ell x = 2\sigma(T_2) + (\ell - 2)x = 2\sigma(T_2) + \ell'x.$$

Thus

$$\sigma(S') + \ell'x = \sigma(S) - 2g + \ell'x = 2\sigma(T_2) - 2g + 2\ell'x = 2\sigma(T_2) - 2g \in 2G.$$

Consequently, if $\Sigma_{\ell'}(2S') = 2G$, then $\sigma(S') + \ell'x \in \Sigma_{\ell'}(2S')$ follows, yielding (22), as desired. Therefore we may assume

$$|\Sigma_{\ell'}(2S')| \leq |2G| - 1 = p - 1. \quad (23)$$

Consequently, since $2G \cong C_p$ has no nontrivial, proper subgroups, we must have $H(\Sigma_{\ell'}(2S'))$ trivial, in which case Theorem 4.2 yields

$$|\Sigma_{\ell'}(2S')| \geq \sum_{y \in 2G} \min\{\ell', v_y(2S')\} - \ell' + 1. \quad (24)$$

Since $\ell' = \ell - 2 \geq p$ holds by (12), we see that if there are 2 distinct terms of $2S'$ each having multiplicity at least $\ell' + 1$, then (24) will contradict (23). Therefore, there is at most one distinct term of $2S'$ having multiplicity at least $\ell' + 1$. Moreover, (24) will again contradict (23) unless such a term of $2S'$ exists having multiplicity at least $2\ell' - p + 2 = 2\ell - p - 2$. Thus

$$h(2S') \geq 2\ell - p - 2 \geq \ell, \quad (25)$$

where the latter inequality follows from (12). In view of our case hypothesis, (16) and (15), it follows that

$$h(2S') \leq h(2S) = v_0(2S) = v_0(S) \leq \ell + 1.$$

Suppose $h(2S) = v_0(2S) = \ell + 1$. Then all nonzero elements will have multiplicity at most $|2S| - \ell - 1 = \ell - 1$ in $2S$, and thus also in $2S'$, while $v_0(2S') \leq v_0(2S) - 2 = \ell - 1$ follows in view of $S' = S \cdot 0^{[-2]} \cdot g^{[-2]}$. In such case, it follows that $h(2S') \leq \ell - 1$, contradicting (25). So we must have $h(2S) = v_0(2S) \leq \ell$. On the other hand, if $h(2S) \leq \ell - 1$, then (25) will again be contradicted in view of the trivial inequality $h(2S') \leq h(2S)$. So we conclude that

$$h(2S) = v_0(2S) = \ell.$$

Now $v_0(2S') \leq v_0(2S) - 2 = \ell - 2$. Thus (25) ensures that there must be a nonzero element having multiplicity at least ℓ in $2S'$, and thus also in $2S$. Since 0 also has multiplicity at least ℓ in $2S$ with $|2S| = |S| = 2\ell$, this is only possible if $|\text{supp}(2S)| = 2$ with both elements from $\text{supp}(2S)$ having multiplicity ℓ in $2S$. As a result, since $\ell \geq p + 2 \geq 3$, the pigeonhole principle guarantees that we can take g with $2g \neq 0$ when defining $S' = S \cdot 0^{[-2]} \cdot g^{[-2]}$, whence $v_0(2S') = v_0(2S) - 2 = \ell - 2$ and $v_{2g}(2S') = v_{2g}(2S) - 2 = \ell - 2$ follow, contradicting (25) for the final time. \square

5. GROUPS WITH A CYCLIC, INDEX 2 SUBGROUP

In this section, we determine the large Davenport constant of all finite groups containing a cyclic, index 2 subgroup. Despite the simple formulation of Theorem 1.1, we will need some specialized information regarding the isomorphism classes of such groups. Thus we summarize their classification in a form suitable for our needs. The main result is Theorem 5.3, which is taken from a recent monograph by Jones, Kwak, and Xu [21, Section 3.4.3]. We start with a lemma which is slightly stronger than the classical result by Hölder. The lemma follows from the characterization given in the above monograph; we have pulled it out for clarity. Hölder's Theorem can be found in [30, Chap. III, §7] or [20, Chapter 7].

Lemma 5.1. *Let G be a finite group of order $|G| = 2n = 2^{s+1}m$, where $\gcd(2, m) = 1$, $s \geq 0$, $m \geq 1$, and $n = 2^s m$. Suppose G has a cyclic, index 2 subgroup. Then G has a presentation of one of the following forms:*

$$(A) \ G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = 1 \rangle,$$

$$(B) \ G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = \alpha^{\frac{1}{2}n} \rangle, \quad \text{or}$$

$$(C) \ G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = \alpha^m \rangle$$

for some $r \in [1, n]$ with (B) only possible if $s \geq 1$. In particular,

$$G = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\} \cup \{\tau, \tau\alpha, \tau\alpha^2, \dots, \tau\alpha^{n-1}\}.$$

Of course, not all values of $r \in [1, n]$ are possible nor necessarily give rise to non-isomorphic groups. However, throughout this section, we will use the format given by Lemma 5.1 for G , saying that G has type (A) if it has a presentation given by (A) in Lemma 5.1, and likewise defining types (B) and (C). Note that if G is of type (C) with $r = 1$, then $\text{ord}(\tau\alpha) = 2n$, which corresponds to when G is cyclic. Also, when $s = 0$, type (C) coincides with type (A), and when $s = 1$, type (C) coincides with type (B).

Type (C) is really only needed when $s \geq 2$, but it will be convenient to state Lemma 5.1 with this slight amount of overlap between types.

In order to unify the notation in the proofs and statements of theorems in this section, we list a set of assumptions regarding hypotheses and notation that we will use throughout this section. The importance of the parameters n^- , n^+ , m^- and m^+ will become apparent later in the section.

General Assumptions for Section 5

- G is a finite group of order $|G| = 2n = 2^{s+1}m$, where $\gcd(2, m) = 1$, $s \geq 0$, $m \geq 1$, and $n = 2^s m$.
- G has a cyclic, index 2 subgroup, notated as in Lemma 5.1, with parameter $r \in [1, n]$.
- $G' = [G, G] \leq G$ is the commutator subgroup of G .
- $P \leq G$ is a Sylow 2-subgroup of G .
- $n^- = \gcd(r-1, n)$ and $n = n^+ n^-$.
- $m^- = \gcd(r-1, m)$ and $m^+ = \gcd(r+1, m)$.

We continue with the characterization for 2-groups, which can be found in many standard texts (e.g., [3, Theorem 1.2]). The general case (Theorem 5.3) follows by routine arguments from the 2-group case.

Lemma 5.2. *Let G satisfy the General Assumptions for Section 5. Suppose G is a 2-group, so $m = 1$ and $G = P$. Then G is isomorphic to one of the following non-isomorphic groups.*

(i) $s \geq 0$ and G is a cyclic group:

$$G \cong C_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha, \quad \tau^2 = \alpha \rangle.$$

(ii) $s \geq 1$ and G is an abelian but non-cyclic group:

$$G \cong C_2 \times C_{2^s} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha, \quad \tau^2 = 1 \rangle.$$

(iii) $s \geq 2$ and G is a dihedral group:

$$G \cong D_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1}, \quad \tau^2 = 1 \rangle.$$

(iv) $s \geq 2$ and G is a generalized quaternion group:

$$G \cong Q_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1}, \quad \tau^2 = \alpha^{2^{s-1}} \rangle.$$

(v) $s \geq 3$ and G is a semi-dihedral group:

$$G \cong SD_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1+2^{s-1}}, \quad \tau^2 = 1 \rangle.$$

(vi) $s \geq 3$ and G is an ordinary meta-cyclic group:

$$G \cong M_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{1+2^{s-1}}, \quad \tau^2 = 1 \rangle.$$

In view of Lemma 5.2, given a finite 2-group P of order 2^{s+1} having a cyclic, index 2 subgroup, we let $\rho(P) \in [1, 2^s]$ be the value of r in its presentation given by Lemma 5.1, i.e.,

$$\rho(P) = \begin{cases} 1, & \text{for } P \text{ given by Lemma 5.2(i)(ii) with } s \geq 0 \\ -1 + 2^s, & \text{for } P \text{ given by Lemma 5.2(iii)(iv) with } s \geq 2 \\ -1 + 2^{s-1}, & \text{for } P \text{ given by Lemma 5.2(v) with } s \geq 3 \\ 1 + 2^{s-1}, & \text{for } P \text{ given by Lemma 5.2(vi) with } s \geq 3. \end{cases}$$

The full classification of finite groups having a cyclic, index 2 subgroup is then the following.

Theorem 5.3. *Let G satisfy the General Assumptions for Section 5. Then the Sylow 2-group P is of one of the six types (i)–(vi) given by Lemma 5.2 and*

$$r \in [1, n] \quad \text{satisfies} \quad r^2 \equiv 1 \pmod{m} \quad \text{and} \quad r \equiv \rho(P) \pmod{2^s}.$$

Furthermore,

1. If P is of type (ii), (iii), (v) or (vi), then G has type (A) in Lemma 5.1.
2. If P is of type (iv), then G has type (B) in Lemma 5.1.
3. If P is of type (i), then G has type (C) in Lemma 5.1.

Different allowed values of $r \in [1, n]$ correspond to non-isomorphic groups, and any group described above indeed has a cyclic, index 2 subgroup.

From Theorem 5.3, we see that the parameter $r \in [1, n]$ must satisfy the equation

$$(r+1)(r-1) = r^2 - 1 \equiv 0 \pmod{m}. \quad (26)$$

Now consider a prime p dividing m . Since p must be odd (as m is odd), either $\gcd(r+1, p) = 1$ or $\gcd(r-1, p) = 1$. Thus (26) implies that either $r+1 \equiv 0 \pmod{p^{v_p(m)}}$ or $r-1 \equiv 0 \pmod{p^{v_p(m)}}$. This means that we can factor

$$\begin{aligned} m &= m^+ m^- \quad \text{with} \quad \gcd(m^+, m^-) = 1, \quad \text{where} \\ m^+ &\geq 1 \quad \text{contains all those primes } p \mid m \text{ with } r+1 \equiv 0 \pmod{p} \quad \text{and} \\ m^- &\geq 1 \quad \text{contains all those primes } p \mid m \text{ with } r-1 \equiv 0 \pmod{p}. \end{aligned} \quad (27)$$

In other words

$$m^+ = \gcd(r+1, m) \quad \text{and} \quad m^- = \gcd(r-1, m).$$

Recall that $n = 2^s m$. Let us next consider the divisibility of $r+1$ and $r-1$ by 2. Given the possibilities for $\rho(P)$, there are five cases, which we summarize below.

$$\begin{array}{llll} v_2(r-1) \geq s & \text{and} & v_2(r+1) \geq s & \text{if } \rho(P) = 1 \text{ with } s \leq 1, \\ v_2(r-1) \geq s & \text{and} & v_2(r+1) = 1 & \text{if } \rho(P) = 1 \text{ with } s \geq 2, \\ v_2(r-1) = 1 & \text{and} & v_2(r+1) \geq s & \text{if } \rho(P) = -1 + 2^s \text{ with } s \geq 2, \\ v_2(r-1) = 1 & \text{and} & v_2(r+1) = s-1 & \text{if } \rho(P) = -1 + 2^{s-1} \text{ with } s \geq 3, \text{ and} \\ v_2(r-1) = s-1 & \text{and} & v_2(r+1) = 1 & \text{if } \rho(P) = 1 + 2^{s-1} \text{ with } s \geq 3. \end{array} \quad (28)$$

Consequently, letting

$$n = n^+ n^- \quad \text{with} \quad n^- = \gcd(r-1, n),$$

we discover that

$$\begin{array}{llll} n^- = 2^s m^- & \text{and} & n^+ = m^+ & \text{if } \rho(P) = 1 \text{ with } s \geq 0, \\ n^- = 2m^- & \text{and} & n^+ = 2^{s-1} m^+ & \text{if } \rho(P) = -1 + 2^s \text{ or } -1 + 2^{s-1} \text{ with } s \geq 2, \text{ and} \\ n^- = 2^{s-1} m^- & \text{and} & n^+ = 2m^+ & \text{if } \rho(P) = 1 + 2^{s-1} \text{ with } s \geq 3. \end{array} \quad (29)$$

Observe that $n^+ \mid r+1$ in all cases, while n^- is even except when $s = 0$. With the above notation in hand, let us now characterize some of the important subgroups of G .

Lemma 5.4. *Let G satisfy the General Assumptions for Section 5. Then*

$$G' = \langle \alpha^{r-1} \rangle = \langle \alpha^{n^-} \rangle \quad \text{and} \quad Z(G) = \begin{cases} G, & \text{if } r = 1 \\ \langle \alpha^{n^+} \rangle, & \text{if } r \neq 1. \end{cases}$$

In particular, G is non-abelian if and only if $r \neq 1$, in which case $|G'| = n^+$ and $|Z(G)| = n^-$.

Proof. Let $\tau^a \alpha^x, \tau^b \alpha^y \in G$ be arbitrary elements, where $a, b \in \{0, 1\}$ and $x, y \in [0, n-1]$. Then

$$\begin{aligned} [\tau^a \alpha^x, \tau^b \alpha^y] &= \alpha^{-x} \tau^{-a} \alpha^{-y} \tau^{-b} \tau^a \alpha^x \tau^b \alpha^y \\ &= \alpha^{-x-r^a y+r^b x+y} = \alpha^{(r^b-1)x-(r^a-1)y}. \end{aligned} \tag{30}$$

Since $r-1$ divides both r^a-1 and r^b-1 , we see from (30) that all commutator elements live in the subgroup $\langle \alpha^{r-1} \rangle$. Moreover, taking $a = y = 1$ and $x = 0$, we see that α^{r-1} is itself a commutator element. This shows that $G' = \langle \alpha^{r-1} \rangle$. In particular, G is abelian if and only if $r = 1$. Moreover, $\text{ord}(\alpha^{r-1}) = \frac{n}{\gcd(r-1, n)} = n^+ = \text{ord}(\alpha^{n^-})$, so that $|G'| = n^+$ and $G' = \langle \alpha^{r-1} \rangle = \langle \alpha^{n^-} \rangle$ (in view of a finite cyclic group of order n containing a unique subgroup of any given order dividing n).

If $r = 1$, then G is abelian and $Z(G) = G$. Let us next determine $Z(G)$ when $r \neq 1$. The element $\tau^a \alpha^x$ lies in the center of G precisely when (30) is equal to 1 for all $b \in \{0, 1\}$ and $y \in [0, n-1]$. If $a = 1$, then the values $b = 0$ and $y = 1$ yield a non-identity value in (30) in view of $r \neq 1$. Therefore $Z(G) \leq \langle \alpha \rangle$. If $a = 0$, then taking the value $b = 1$ in (30) shows that only values $x \in [0, n-1]$ with $(r-1)x \equiv 0 \pmod n$ can correspond to elements of the center. Hence we must have $x \equiv 0 \pmod{n^+}$, which means that $Z(G) \leq \langle \alpha^{n^+} \rangle$. However, it is easily seen from (30) that $\alpha^{n^+} \in Z(G)$, whence $Z(G) = \langle \alpha^{n^+} \rangle$. Since $\text{ord}(\alpha^{n^+}) = n^-$, we have $|Z(G)| = n^-$. \square

The following lemma gives a non-cyclic subgroup isomorphic to $C_2 \times C_{n^-}$ in most cases, which can then be combined with Theorem 3.2 to bound $D(G)$.

Lemma 5.5. *Let G satisfy the General Assumptions for Section 5. If P is neither cyclic nor dicyclic, then*

$$C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle \cong C_2 \times C_{n^-} \quad \text{is non-cyclic.}$$

Proof. Since P is neither cyclic nor dicyclic, Theorem 5.3 shows that G must have type (A) with $s \geq 1$. In view of (29) and $s \geq 1$, we have n^- even, whence $C_2 \times C_{n^-}$ is non-cyclic.

Let $\tau^a \alpha^x \in G$ be arbitrary, where $a \in \{0, 1\}$ and $x \in [0, n-1]$. Then

$$[\tau, \tau^a \alpha^x] = \tau^{-1} \alpha^{-x} \tau^{-a} \tau \tau^a \alpha^x = \alpha^{-(r-1)x}. \tag{31}$$

Now (31) is equal to 1 precisely when $x \equiv 0 \pmod{n^+}$, which means that $C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle$ with $|C_G(\tau)| = 2n^-$. In view of Lemma 5.4, we know $\alpha^{n^+} \in Z(G)$, which forces $C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle$ to be abelian. Consequently, since $\text{ord}(\alpha^{n^+}) = n^-$ and $|C_G(\tau)| = 2n^-$, we conclude that $C_G(\tau)$ is isomorphic to either $C_2 \times C_{n^-}$ or C_{2n^-} . Thus to complete the proof, we simply need to show that

$$\text{ord}(\tau \alpha^{x n^+}) < 2n^- \quad \text{for all } x \in [0, n^- - 1].$$

To this end, let $x \in [0, n^- - 1]$ be arbitrary. Since G has type (A), we have

$$(\tau\alpha^{xn^+})^2 = \alpha^{(r+1)xn^+} \quad \text{with} \quad \text{ord}(\tau\alpha^{xn^+}) = 2 \text{ord}(\alpha^{(r+1)xn^+}). \quad (32)$$

Recall that n^- is even (in view of $s \geq 1$), that $m^+ \mid n^+$, that $m^- \mid n^-$ and that $m^+m^- = m$ is odd. Thus

$$\frac{1}{2}n^-(r+1)xn^+ \equiv m^-m^+ \equiv m \equiv 0 \pmod{m}.$$

As a result, $\text{ord}(\alpha^{(r+1)xn^+}) \leq \frac{1}{2}n^-$ will follow, proving that $C_G(\tau)$ is non-cyclic in view of (32), provided

$$\mathbf{v}_2\left(\frac{1}{2}n^-(r+1)n^+\right) = \mathbf{v}_2((r+1)n) - 1 \geq s = \mathbf{v}_2(n),$$

i.e., provided $\mathbf{v}_2(r+1) \geq 1$. However, in view of (28) and $s \geq 1$, we see that this is indeed the case, completing the proof. \square

Next, we give the lower bound for $D(G)$.

Lemma 5.6. *Let G satisfy the General Assumptions for Section 5. Then*

$$\frac{1}{2}|G| + |G'| \leq D(G).$$

Proof. From Lemma 5.4, we know $|G'| = n^+$. Consider the sequence

$$U = (\tau^{-1}\alpha) \cdot \alpha^{[n^+-1]} \cdot (\tau\alpha^{1-n^+}) \cdot \alpha^{[n-1]} \in \mathcal{F}(G).$$

Then $|U| = n + n^+ = \frac{1}{2}|G| + |G'|$. Since $(\tau^{-1}\alpha)\alpha^{n^+-1}(\tau\alpha^{1-n^+})\alpha^{n-1} = 1$ —as is easily seen by recalling from Lemma 5.4 that $\alpha^{n^+} \in Z(G)$ —it is clear that U is a product-one sequence. Thus to complete the proof, we need to show that $U \in \mathcal{A}(G)$ is an atom.

Assume to the contrary that we have a factorization $U = V \cdot W$ with $V, W \in \mathcal{B}(G)$ both nontrivial. Since V and W are product-one sequences, we have (without restriction) $V \in \mathcal{F}(\langle \alpha \rangle)$ and $(\tau^{-1}\alpha) \cdot (\tau\alpha^{1-n^+}) \mid W$. Hence $V = \alpha^{[n]}$ and $W = \alpha^{[n^+-2]} \cdot (\tau^{-1}\alpha) \cdot (\tau\alpha^{1-n^+})$. Thus there exists a $k \in [0, n^+ - 2]$ such that $1 = (\tau^{-1}\alpha)\alpha^k(\tau\alpha^{1-n^+})\alpha^{n^+-2-k} \in \pi(W)$ —in view of Lemma 2.3, cyclically shifting the terms in a product-one ordered sequence preserves that the sequence has product-one, so we can w.l.o.g. assume our product-one expression starts with $\tau^{-1}\alpha$. Since $1 = (\tau^{-1}\alpha)\alpha^k(\tau\alpha^{1-n^+})\alpha^{n^+-2-k} = \alpha^{(r-1)(k+1)}$, it follows that $k+1 \in [1, n^+ - 1]$ must be a multiple of $\text{ord}(\alpha^{r-1})$. However, since $n^- = \gcd(r-1, n)$ with $n = n^+n^-$, it follows that $\text{ord}(\alpha^{r-1}) = n^+$, so that $k+1 \in [1, n^+ - 1]$ cannot be a multiple of $\text{ord}(\alpha^{r-1})$. This contradiction establishes the desired lower bound for $D(G)$. \square

The next lemma reduces the problem of finding a matching upper bound for $D(G)$ to the case when $|G'| = n^+$ is prime.

Lemma 5.7. *Let G satisfy the General Assumptions for Section 5. Suppose G is non-abelian, let p be a prime divisor of $|G'| = n^+$, and let*

$$H = \langle \alpha^{\frac{n^+}{p}}, \tau \rangle \leq G.$$

Then H has a cyclic, index 2 subgroup and $|H'| = p$, where $H' = [H, H] \leq H$ is the commutator subgroup of H . In particular, if $D(H) \leq \frac{1}{2}|H| + |H'|$, then $D(G) \leq \frac{1}{2}|G| + |G'|$.

Proof. Observe that $\text{ord}(\alpha^{\frac{n^+}{p}}) = \text{ord}(\alpha)^{\frac{p}{n^+}} = n^-p$. If G has type (A), then $\tau^2 = 1 \in \langle \alpha^{\frac{n^+}{p}} \rangle$. If G has type (B), then $s \geq 1$ and n^- is even. Thus $\tau^2 = \alpha^{\frac{n}{2}} \in \langle \alpha^{\frac{n^+}{p}} \rangle$ since $(\frac{n^+}{p})\frac{pn^-}{2} = \frac{n}{2}$ with $2 \mid n^-$. If G has type (C), then P is cyclic. Hence (29) implies that $m^+ = n^+$, and now $\tau^2 = \alpha^m \in \langle \alpha^{\frac{n^+}{p}} \rangle$ holds in view of $(\frac{n^+}{p})m^-p = \frac{m^+m^-p}{p} = m$. In all cases, we conclude that

$$|H| = 2 \text{ord}(\alpha^{\frac{n^+}{p}}) = 2n^-p,$$

so that $\langle \alpha^{\frac{n^+}{p}} \rangle \leq H$ is a cyclic, index 2 subgroup.

Next, let us compute $H' \leq H$. Let $\tau^a \alpha^x, \tau^b \alpha^y \in H$ be arbitrary elements, where $a, b \in \{0, 1\}$, $x, y \in [0, n-1]$ and $x \equiv y \equiv 0 \pmod{\frac{n^+}{p}}$. Then (as in Lemma 5.4)

$$[\tau^a \alpha^x, \tau^b \alpha^y] = \alpha^{(r^b-1)x - (r^a-1)y}. \quad (33)$$

Since $x \equiv y \equiv 0 \pmod{\frac{n^+}{p}}$ and since $r-1$ divides both r^b-1 and r^a-1 , we see from (33) that all commutator elements live in the subgroup $\langle \alpha^{(r-1)\frac{n^+}{p}} \rangle$. Moreover, taking $a=1, y=\frac{n^+}{p}$ and $x=0$, we see that $\alpha^{(r-1)\frac{n^+}{p}}$ is itself a commutator element. This shows that $H' = \langle \alpha^{(r-1)\frac{n^+}{p}} \rangle$. In consequence, since $\gcd(r-1, n) = n^-$ and $n = n^+n^-$, it follows that $|H'| = p$.

Now $|H| = 2n^-p, |H'| = p, |G'| = n^+$ (from Lemma 5.4) and $|G : H| = \frac{2n}{2n^-p} = \frac{n^+}{p}$. Thus, if $D(H) \leq \frac{1}{2}|H| + |H'|$, then Theorem 3.2 yields

$$D(G) \leq D(H)|G : H| \leq (\frac{1}{2}|H| + |H'|)|G : H| = \frac{1}{2}|G| + |H'||G : H| = n + n^+ = \frac{1}{2}|G| + |G'|. \quad \square$$

The following lemma handles the case when there are a sufficient number of terms from $\langle \alpha \rangle$.

Lemma 5.8. *Let G satisfy the General Assumptions for Section 5. Suppose $n^+ = p$ is prime and let $U \in \mathcal{F}(G)$ be a product-one sequence. If $|U| \geq n + p + 1$ and U contains at least $p-1$ terms from $\langle \alpha \rangle \setminus Z(G)$, then U is not an atom.*

Proof. Since $n^+ = p$ is prime, we have $n^+ = p \geq 2$. Thus Lemma 5.4 implies that G is non-abelian with $Z(G) = \langle \alpha^{n^+} \rangle = \langle \alpha^p \rangle$ and $G' = \langle \alpha^{n^-} \rangle = \langle \alpha^{r-1} \rangle$. In particular, $|G'| = n^+ = p \geq 2$ and $|Z(G)| = n^-$.

By hypothesis, there is a subsequence $V \mid U$ with $\text{supp}(V) \subset \langle \alpha \rangle \setminus Z(G)$ and $|V| = p-1$, say $V = v_1 \cdot \dots \cdot v_{p-1}$ with

$$v_i = \alpha^{x_i} \quad \text{for } i \in [1, p-1],$$

where $x_i \in [0, n-1]$. Since $v_i \notin Z(G) = \langle \alpha^p \rangle$ for all $i \in [1, p-1]$, we see that

$$x_i \not\equiv 0 \pmod{p} \quad \text{for all } i \in [1, p-1]. \quad (34)$$

If $\text{supp}(U) \subset \langle \alpha \rangle$, then $|U| \geq n + p + 1 > n = |\langle \alpha \rangle| \geq D(\langle \alpha \rangle)$ ensures that U cannot be an atom, as desired, where the final inequality follows from Lemma 2.4. Therefore we can assume there is some $z = \tau \alpha^x \in \text{supp}(U)$ with $x \in [0, n-1]$.

As remarked in Section 2, $\pi(V \cdot z)$ is contained in a G' -coset. Let us next show that

$$|\pi(V \cdot z)| = p = |G'|, \quad (35)$$

so that $\pi(V \cdot z)$ is an entire G' -coset.

Let W^* be an ordering of the terms of $V \cdot z$, so $W^* \in \mathcal{F}^*(G)$ with $[W^*] = V \cdot z$. Then

$$\pi(W^*) = \tau \alpha^{x + \sum_{i=1}^{p-1} \epsilon_i x_i}, \quad (36)$$

where $\epsilon_i = 1$ if the term x_i occurs to the right of $z = \tau \alpha^x$ in W^* , and $\epsilon_i = r$ if the term x_i occurs to the left of $z = \tau \alpha^x$ in W^* . The possible exponents for α in (36) (as we range over all possible orderings W^* of $V \cdot z$) are then

$$x + \{x_1, rx_1\} + \dots + \{x_{p-1}, rx_{p-1}\} = x + \sum_{i=1}^{p-1} x_i + \{0, (r-1)x_1\} + \dots + \{0, (r-1)x_{p-1}\}.$$

Consequently,

$$\pi(V \cdot z) = \tau \alpha^{x + \sum_{i=1}^{p-1} x_i} \{(\alpha^{r-1})^y : y \in Y\}, \quad (37)$$

where $Y = \{0, x_1\} + \dots + \{0, x_{p-1}\}$. Recall that α^{r-1} is a generator for G' having $\text{ord}(\alpha^{r-1}) = n^+ = p$. Thus the cardinality of $\pi(V \cdot z)$ is just the number of residue classes modulo p in $Y = \{0, x_1\} + \dots + \{0, x_{p-1}\}$. From (34), we see that each set $\{0, x_i\}$ consists of 2 elements that are distinct modulo p , in which case applying the Cauchy-Davenport Theorem to Y shows that $|Y| = p = |G'|$, which combined with (37) establishes (35), as claimed.

Now $|U \cdot (V \cdot z)^{-1}| = |U| - p \geq n + 1 = d(G) + 1$, with the first inequality by hypothesis and the final equality from Theorem 3.1. Thus we can apply the definition of $d(G)$ to $U \cdot (V \cdot z)^{-1}$ to find a nontrivial, product-one subsequence $T \mid U \cdot (V \cdot z)^{-1}$. But now Lemma 2.2 shows that $\pi(U \cdot T^{[-1]}) \subset G'$. As a result, since $V \cdot z \mid U \cdot T^{[-1]}$ follows from the definition of T , it follows in view of (35) that $\pi(U \cdot T^{[-1]}) = G'$. In particular, $1 \in G' = \pi(U \cdot T^{[-1]})$. Thus $U = (U \cdot T^{[-1]}) \cdot T$ is a factorization of U into two nontrivial, product-one subsequences, ensuring that U is not an atom, as desired. \square

When either n^+ or n^- is too small, the general strategy for proving Theorem 1.1 breaks down, requiring the cases when $n^- \leq 2$ or $n^+ \leq 2$ to be handled separately. Most of these remaining cases can be handled by simple arguments. However, the case when G is isomorphic to a dicyclic group Q_{4p} with p odd is particularly difficult, so we handle it separately now.

Lemma 5.9. *Let G be a dicyclic group of order $4p$ with p an odd prime, say*

$$G = Q_{4p} = \langle \alpha, \tau \mid \alpha^{2p} = 1, \quad \tau^2 = \alpha^p, \quad \alpha\tau = \tau\alpha^{-1} \rangle.$$

Then $D(G) \leq \frac{1}{2}|G| + |G'| = 3p$, where $G' = [G, G] \leq G$ is the commutator subgroup.

Proof. By hypothesis, G satisfies the Standard Assumptions of Section 5 having types (B) and (C) (since these types coincide for $s = 1$) with

$$s = 1, \quad P \leq G \text{ cyclic}, \quad n = 2p, \quad r = 2p - 1, \quad n^- = 2, \quad m^- = 1, \quad \text{and} \quad n^+ = m^+ = p.$$

As a result, Lemma 5.4 tells us that

$$G' = \langle \alpha^2 \rangle \cong C_p \quad \text{and} \quad Z(G) = \langle \alpha^p \rangle \cong C_2. \quad (38)$$

Assume by contradiction that we have some atom $U \in \mathcal{A}(G)$ with $|U| = D(G) \geq 3p + 1$. Since U is a product-one sequence, there is an ordering of its terms with product 1, say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$ and $\pi(U^*) = 1$.

Suppose $Z(G) \cap \text{supp}(U) \neq \emptyset$. Since U is an atom and G is nontrivial, we cannot have $1 \in \text{supp}(U)$. Thus, in view of (38) and $Z(G) \cap \text{supp}(U) \neq \emptyset$, we must have $\alpha^p \in \text{supp}(U)$. By Lemma 2.3, we can w.l.o.g. assume α^p is equal to the first term of U^* , so $U^*(1) = \alpha^p$. But then $|U^*(2, |U| - 1)| = |U| - 2 \geq 3p - 1 \geq 2p = |G/Z(G)|$, which means we can apply Lemma 2.4 to $\phi_{Z(G)}(U^*(2, |U| - 1))$ and thereby find a nontrivial, consecutive subsequence of $U^*(2, |U| - 1)$ with product from $Z(G) = \{1, \alpha^p\}$, say $U^*(I)$ with $I \subset [2, |U| - 1]$ an interval. Since $U = [U^*] \in \mathcal{A}(G)$ is an atom, Lemma 2.1 ensures that $\pi(U^*(I)) \neq 1$. Thus $\pi(U^*(I)) = \alpha^p \in Z(G)$ with $U^*(I) \mid U^*(2, |U| - 1)$ consecutive, in which case $\pi(U^*(1) \cdot U^*(I) \cdot U^*([2, |U|] \setminus I)) = \pi(U^*) = 1$. However, $\pi(U^*(1) \cdot U^*(I)) = \alpha^p \alpha^p = \alpha^{2p} = 1$, so that $U = [U^*] = [U^*(1) \cdot U^*(I)] \cdot [U^*([2, |U|] \setminus I)]$ is a factorization of U into 2 nontrivial, product-one subsequences—the subsequence $[U^*([2, |U|] \setminus I)]$ is nontrivial since $I \subset [2, |U| - 1]$ —contradicting that $U \in \mathcal{A}(G)$ is an atom in this case as well. So we instead conclude that

$$Z(G) \cap \text{supp}(U) = \emptyset. \quad (39)$$

In view of Lemma 5.8 and (39), we may assume

$$\text{there are at most } p - 2 \text{ terms of } U \text{ from } \langle \alpha \rangle. \quad (40)$$

Let $J \subset [1, |U|]$ be all those indices $j \in [1, |U|]$ with $U^*(j) \in \tau\langle \alpha \rangle$. Since $\pi(U^*) = 1$, it is easily deduced from the group presentation for G that $|J|$ must be even. In view of (40), we have $|J| \geq |U| - p + 2 \geq 2p + 3$. Thus, since $|J|$ must be even, it follows that

$$|J| \geq 2p + 4. \quad (41)$$

Let

$$j_1 < j_2 < \dots < j_{2w-1} < j_{2w}$$

be the distinct elements of J , where

$$w = \frac{1}{2}|J| \geq p + 2.$$

In view of Lemma 2.3, we can cyclically shift the ordering U^* of U until the first term of U^* is from $\tau\langle \alpha \rangle$, i.e., such that $j_1 = 1$.

Now define an ordered sequence

$$U'^* = U^*(j_1, j_2 - 1) \cdot U^*(j_2, j_3 - 1) \cdot \dots \cdot U^*(j_{2w-1}, j_{2w} - 1) \cdot U^*(j_{2w}, |U|) \in \mathcal{F}^*(G).$$

The ordered sequence U'^* is obtained from the product-one ordered sequence U^* by repeatedly replacing a consecutive subsequence with a single term equal to its product. As noted in Section 2, since $[U^*] = U \in \mathcal{A}(G)$ was an atom, this ensures that

$$U' := [U'^*] \in \mathcal{A}(G)$$

is also an atom. From the definition of the j_i , each $U^*(j_i, j_{i+1} - 1)$, for $i \in [1, 2w]$ where $j_{2w+1} = |U| + 1$, has its first term from $\tau\langle \alpha \rangle$ and all other terms from $\langle \alpha \rangle$. In consequence, we have

$$\text{supp}(U') \subset \tau\langle \alpha \rangle \quad \text{and} \quad |U'| = |J| = 2w \geq 2p + 4,$$

where the inequality follows from (41).

Define a map $\bar{\cdot} : \tau\langle\alpha\rangle \rightarrow \mathbb{Z}/2p\mathbb{Z}$ by setting $\overline{\tau\alpha^x} := \phi_{2p\mathbb{Z}}(x) \in \mathbb{Z}/2p\mathbb{Z}$, i.e., $\tau\alpha^x$ maps to the residue class represented by x modulo p . Since $\text{ord}(\alpha) = 2p$, the map $\bar{\cdot}$ is well-defined. We continue with a straightforward claim.

Claim A. Let $R \in \mathcal{F}(G)$ with $\text{supp}(R) \subset \tau\langle\alpha\rangle$. Then R is a product-one sequence precisely when there exists a factorization $R = R^+ \cdot R^-$ such that $|\overline{R^+}| = |\overline{R^-}|$ and $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p$.

Proof. Suppose R is a product-one sequence. Then there exists an ordering of R , say $R^* \in \mathcal{F}^*(G)$ with $[R^*] = R$, such that $\pi(R^*) = 1$. Since $\pi(R^*) = 1$ and $\text{supp}(R) \subset \tau\langle\alpha\rangle$, it is easily deduced from the group presentation for G that $|R|$ must be even. Thus let

$$R^* = (\tau\alpha^{r_1^-}) \cdot (\tau\alpha^{r_1^+}) \cdot \dots \cdot (\tau\alpha^{r_w^-}) \cdot (\tau\alpha^{r_w^+}) \in \mathcal{F}^*(G),$$

where $r_i^-, r_i^+ \in [0, 2p-1]$ and $w = \frac{1}{2}|R|$. Repeatedly applying the group presentation relations for G yields

$$1 = \pi(R^*) = (\tau\alpha^{r_1^-} \tau\alpha^{r_1^+})(\tau\alpha^{r_2^-} \tau\alpha^{r_2^+}) \dots (\tau\alpha^{r_w^-} \tau\alpha^{r_w^+}) = \alpha^{wp + \sum_{i=1}^w r_i^+ - \sum_{i=1}^w r_i^-}, \quad (42)$$

thus implying

$$wp + \sum_{i=1}^w r_i^+ - \sum_{i=1}^w r_i^- \equiv 0 \pmod{2p}. \quad (43)$$

Let

$$R^- = [R^*(I^-)] = (\tau\alpha^{r_1^-}) \cdot \dots \cdot (\tau\alpha^{r_w^-}) \quad \text{and} \quad R^+ = [R^*(I^+)] = (\tau\alpha^{r_1^+}) \cdot \dots \cdot (\tau\alpha^{r_w^+}),$$

where $I^- = \{1, 3, \dots, 2w-1\}$ and $I^+ = \{2, 4, \dots, 2w\}$. Since $I^- \cup I^+ = [1, 2w] = [1, |R|]$ with the union disjoint, we see that $R = R^+ \cdot R^-$ with $|\overline{R^-}| = |R^-| = |R^+| = |\overline{R^+}| = w = \frac{1}{2}|R|$. Moreover, (43) is equivalent to saying $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = wp = \frac{1}{2}|R|p$. Thus one direction of the claim is established.

Now suppose that we have a factorization $R = R^+ \cdot R^-$ such that $|\overline{R^+}| = |\overline{R^-}|$ and $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p$. Let $R^* \in \mathcal{F}^*(G)$ be an ordering of R such that $[R^*(I^-)] = R^-$ and $[R^*(I^+)] = R^+$, where $I^- \subset [1, |R|]$ is the subset of odd indices and $I^+ \subset [1, |R|]$ is the subset of even indices. Since $R = R^+ \cdot R^-$ with $|R^+| = |\overline{R^+}| = |\overline{R^-}| = |R^-|$, it follows that $|R|$ is even, so that $|I^+| = |I^-| = \frac{1}{2}|R|$. Let $w = \frac{1}{2}|R|$ and let

$$R^*(2i-1) = \tau\alpha^{r_i^-} \quad \text{and} \quad R^*(2i) = \tau\alpha^{r_i^+} \quad \text{for } i \in [1, \frac{1}{2}|R|] = [1, w].$$

Then, in view of $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p = wp$, we see that (43) holds, and consequently also (42). Thus $1 = \pi(R^*) \in \pi([R^*]) = \pi(R)$, showing that R is a product-one sequence, which completes the claim. \square

Using Claim A, we see that Lemma 4.3 is equivalent to saying that the maximal length of an atom $V \in \mathcal{A}(G)$ with $\text{supp}(V) \subset \tau\langle\alpha\rangle$ is $|V| \leq 2p+3$. However, this contradicts that we constructed above an atom $U' \in \mathcal{A}(G)$ with $\text{supp}(U') \subset \tau\langle\alpha\rangle$ and $|U'| \geq 2p+4$, completing the proof. \square

With the above preparatory work complete, we are now ready to begin the proof of Theorem 1.1

Proof of Theorem 1.1. If G is cyclic, then $d(G) = |G| - 1$, while $d(G) = \frac{1}{2}|G|$ follows for non-cyclic G having a cyclic, index 2 subgroup, and if G is abelian, then $D(G) = d(G) + 1$ (by Lemma 2.4 and Theorem 3.1).

Therefore we may assume G is non-abelian and satisfies the General Assumptions for Section 5. Lemma 5.6 gives $d(G) + |G'| = \frac{1}{2}|G| + |G'| \leq D(G)$. Since G is non-abelian, Lemma 5.4 gives $|G'| = n^+ \geq 2$, and it remains to show the upper bound

$$D(G) \leq \frac{1}{2}|G| + |G'| = n + n^+. \quad (44)$$

By Lemma 5.7, it suffices to prove (44) when $|G'| = n^+ = p$ is prime. Furthermore, if $n^+ = 2$, then Lemma 3.4 yields (44). Consequently, we can assume

$$|G'| = n^+ = p \geq 3 \quad \text{is prime.} \quad (45)$$

In particular, only the cases where $n^+ = p$ is odd remain, which in view of (29) means that $\rho(P) = 1$. From the definition of ρ , we see that $\rho(P) = 1$ corresponds to when $P \cong C_{2s+1}$ or $P \cong C_2 \times C_{2s}$. However, if $P \cong C_2 \times C_{2s}$ is non-cyclic, then Lemma 5.5 shows that $C_G(\tau) \cong C_2 \times C_{n^-}$ is non-cyclic. Since $D(C_2 \times C_{n^-}) = n^- + 1$ is well-known ([14, Theorem 5.8.3]), invoking Theorem 3.2 would then yield

$$D(G) \leq D(C_G(\tau))|G : C_G(\tau)| = D(C_2 \times C_{n^-})n^+ = (n^- + 1)n^+ = n + n^+,$$

yielding (44). So it remains to prove (44) when

$$P \cong C_{2s+1} \quad \text{is cyclic with } \rho(P) = 1.$$

In particular, Theorem 5.3 now tells us that G has type (C).

If $n^- = 1$, then (29) and the definition of n^- and m^- ensure that $s = 0$, $r = n - 1$ and $p = n^+ = n$. This corresponds to the case when G is dihedral of order $2n$ with n odd. In this case, Lemma 2.4 implies $D(G) \leq |G| = 2n = n + n^+$, yielding (44). Therefore we may assume $n^- \geq 2$.

Suppose $n^- = 2$. Then it follows in view of $\rho(P) = 1$ and (29) that

$$s = 1, \quad m^- = 1, \quad n^+ = m^+ = m = p \quad \text{and} \quad n = 2m = 2p.$$

Since P is cyclic with $s = 1$, Theorem 5.3 ensures that G has types (C) and (B) (these types coincide for $s = 1$) with

$$(r - 1)(r + 1) = r^2 - 1 \equiv 0 \pmod{m} \quad \text{and} \quad r \equiv 1 \pmod{2}.$$

In consequence, since $1 = m^- = \gcd(r - 1, m)$ and $r \in [1, n]$, it follows that $r = n - 1 = 2p - 1$. As a result, we see that $G \cong Q_{4p}$ is dicyclic, in which case Lemma 5.9 yields (44). So we may assume

$$n^- \geq 3. \quad (46)$$

To establish (44), assume by contradiction that we have an atom $U \in \mathcal{A}(G)$ with

$$|U| = D(G) \geq n + n^+ + 1 = n^+n^- + n^+ + 1. \quad (47)$$

Factor $U = U_\alpha \cdot U_\tau$ with $\text{supp}(U_\alpha) \subset \langle \alpha \rangle$ and $\text{supp}(U_\tau) \subset \tau \langle \alpha \rangle$. In view of Lemma 5.4, we know

$$Z(G) = \langle \alpha^{n^+} \rangle = \langle \alpha^p \rangle \quad \text{and} \quad G' = \langle \alpha^{n^-} \rangle = \langle \alpha^{r-1} \rangle \quad \text{with} \quad |G'| = n^+ = p.$$

Let $U'_\alpha \mid U_\alpha$ be the subsequence consisting of all terms from $\langle \alpha \rangle \setminus Z(G)$. Then, since $Z(G) = \langle \alpha^p \rangle$, we see that $U_\alpha \cdot U'_\alpha{}^{[-1]}$ is the subsequence of U consisting of all terms from $Z(G)$.

Let us next show that

$$|U'_\alpha| \leq n^+ - 2, \quad |U_\alpha \cdot U'_\alpha{}^{[-1]}| \leq n^- - 1 \quad \text{and} \quad |U_\alpha| \leq n^+ + n^- - 3. \quad (48)$$

In view of Lemma 5.8, we have $|U'_\alpha| \leq n^+ - 2$. Thus, if (48) fails, then we must have $|U_\alpha \cdot U'_\alpha{}^{[-1]}| = |U_\alpha| - |U'_\alpha| \geq n^-$. In other words, there are at least $n^- = |Z(G)|$ terms of U from $Z(G)$. Since $U \in \mathcal{A}(G)$ is an atom, let $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$ be an ordering of U such that $\pi(U^*) = 1$. Any term from $Z(G)$ can be moved around in the ordered sequence U^* without changing the value of $\pi(U^*)$. Thus we can w.l.o.g. assume all terms from $U_\alpha \cdot U'_\alpha{}^{[-1]}$ are consecutive in U^* . In consequence, since $|U_\alpha \cdot U'_\alpha{}^{[-1]}| \geq |Z(G)| = n^-$, we can apply Lemma 2.4 to $U_\alpha \cdot U'_\alpha{}^{[-1]}$ to find a nontrivial, consecutive, product-one subsequence $U^*(I)$, where $I \subset [1, |U|]$ is an interval. Moreover, $|U^*(I)| \leq |Z(G)| = n^- < |U|$, meaning $U^*(I) \mid U$ is proper. But since $U = [U^*] \in \mathcal{A}(G)$ is an atom, this contradicts Lemma 2.1. So (48) is established, as claimed.

Define a map $\iota : G \rightarrow \mathbb{Z}$ by setting

$$\iota(\tau^y \alpha^x) = x, \quad \text{where } x \in [0, n-1] \text{ and } y \in [0, 1],$$

and define a map $\bar{\cdot} : G \rightarrow \mathbb{Z}/p\mathbb{Z}$ by setting

$$\bar{g} = \phi_{p\mathbb{Z}}(\iota(g)) \quad \text{for } g \in G,$$

so $g = \tau^y \alpha^x \in G$ maps to the residue class modulo p given by $\iota(g) = x$.

Let $R \in \mathcal{F}(G)$ be a sequence and let $R^* \in \mathcal{F}^*(G)$ be an arbitrary ordering of R , so $[R^*] = R$. Factor $R = R_\alpha \cdot R_\tau$ with $\text{supp}(R_\alpha) \subset \langle \alpha \rangle$ and $\text{supp}(R_\tau) \subset \tau \langle \alpha \rangle$. We proceed to describe $\pi(R)$ under the assumption that

$$|R_\tau| \geq 1.$$

First note that, from the defining relations for G , it is clear that $\pi(R^*) \in \langle \alpha \rangle$ if and only if the number of terms of R from $\tau \langle \alpha \rangle$ is even, that is, if $|R_\tau|$ is even. Let $\omega = \lfloor \frac{1}{2}|R_\tau| \rfloor$, so that $|R_\tau| = 2\omega$ when $\pi(R^*) \in \langle \alpha \rangle$ and $|R_\tau| = 2\omega + 1$ when $\pi(R^*) \in \tau \langle \alpha \rangle$.

Next, since G has type (C), a routine application of the defining relations for G shows that

$$\pi(R^*) = \tau^\epsilon \alpha^{\omega m + \sum_{i=1}^{|R|} d_i \iota(R^*(i))}, \quad (49)$$

where $\epsilon = 1$ if $|R_\tau|$ is odd, $\epsilon = 0$ if $|R_\tau|$ is even, $d_i = 1$ if the number of terms of R^* from $\tau \langle \alpha \rangle$ to the right of $R^*(i)$ is even, and $d_i = r$ if the number of terms of R^* from $\tau \langle \alpha \rangle$ to the right of $R^*(i)$ is odd.

There are some important consequences of the formula (49). Let $I \subset [1, |R|]$ be the set of indices such that $[R^*(I)] = R_\tau$. If we fix the position of every term $R^*(i) \in \langle \alpha \rangle$ with $i \notin I$ but allow ourselves to permute the terms within $R^*(I)$, this maintains that $[R^*(I)] = R_\tau$ while each coefficient d_i , for $i \in [1, |R|] \setminus I$, remains unaffected and constant. In consequence, when trying to determine the possible values for (49) over all orderings R^* , we can first decide how to distribute the terms from R_α into R^* , thus fixing and determining the subset of indices $I \subset [1, |R|]$ with $[R^*(I)] = R_\tau$, and then decide how to permute the terms within $R^*(I)$. Since $|R_\tau| \geq 1$, every term of R_α can either be placed in R^* such that the number of terms of R^* from $\tau \langle \alpha \rangle$ to its right is even, or such that this number is odd. Changing this choice has the effect on (49) of switching d_i between 1 and r . Once we have fixed how the terms of R from $\langle \alpha \rangle$ are to be distributed in R^* , the set $I \subset [1, |R|]$ is then fixed, but we are free to re-order the terms from R_τ so long as we preserve $[R^*(I)] = R_\tau$ and this will not affect whether $d_i = 1$ or $d_i = r$ holds for any $i \in [1, |R|] \setminus I$.

Concerning the terms of R^* from R_τ , whether $d_i = 1$ or $d_i = r$ holds for $i \in I$ depends entirely on whether $R^*(i) = (R^*(I))(j)$ with $j \equiv \epsilon \pmod{2}$ or $j \equiv \epsilon - 1 \pmod{2}$. If $j \equiv \epsilon \pmod{2}$, then $d_i = 1$, and if $j \equiv \epsilon - 1 \pmod{2}$, then $d_i = r$. Letting

$$J = \{1 + \epsilon, 3 + \epsilon, \dots, 2\omega - 1 + \epsilon\} \subset [1, |R_\tau|]$$

be the subset of indices congruent to $\epsilon - 1$ modulo 2, we are free to arrange for $[(R^*(I))(J)]$ to be any subsequence of R_τ having length $\omega = \lfloor \frac{1}{2}|R_\tau| \rfloor$, and then $d_i = r$ will hold for all these terms, while $d_i = 1$ will hold for all remaining terms of R_τ .

In summary, the above works shows that

$$\pi(R) = \tau^\epsilon \alpha^{\omega m} \{\alpha^x : x \in X\},$$

where

$$\begin{aligned} X &= \sum_{i=1}^{|R_\alpha|} \left\{ \iota(R_\alpha^*(i)), r \iota(R_\alpha^*(i)) \right\} + \left\{ r \sigma(\iota(R'_\tau)) + \sigma(\iota(R_\tau \cdot R'_\tau)^{[-1]}) : R'_\tau \mid R_\tau, |R'_\tau| = \omega = \left\lfloor \frac{1}{2}|R_\tau| \right\rfloor \right\} \\ &= \sigma(\iota(R)) + (r-1) \left(\{0, \iota(R_\alpha^*(1))\} + \dots + \{0, \iota(R_\alpha^*(|R_\alpha|))\} + \Sigma_{\lfloor \frac{1}{2}|R_\tau| \rfloor}(\iota(R_\tau)) \right) \end{aligned}$$

and $R_\alpha^* \in \mathcal{F}^*(G)$ is any ordering of R_α . Consequently,

$$\pi(R) = \tau^\epsilon \alpha^{xm + \sigma(\iota(R))} \{(\alpha^{r-1})^y : y \in Y\}, \quad (50)$$

where

$$Y = \{0, \iota(R_\alpha^*(1))\} + \dots + \{0, \iota(R_\alpha^*(|R_\alpha|))\} + \Sigma_{\lfloor \frac{1}{2}|R_\tau| \rfloor}(\iota(R_\tau)).$$

Since $\text{ord}(\alpha^{r-1}) = \text{ord}(\alpha^{n^-}) = n^+ = p$, we conclude that $|\pi(R)|$ is equal to the number of distinct residue classes modulo p in Y .

Let us next apply some of the above reasoning to the sequence U in the following claim, which shows that any sufficiently small subsequence can be placed in an ordering of U with product one so as to avoid some long length, consecutive subsequence.

Claim A. If $T \mid U$ is a subsequence with $|T| \leq n^+ - 1$, then there exists an ordering of U , say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, and an interval $J \subset [1, |U|]$ such that $\pi(U^*) = 1$, $T \mid [U^*]([1, |U|] \setminus J)$ and $|J| \geq 2n^-$.

Proof. Since $U \in \mathcal{A}(G)$ is an atom, there is an ordering of U , say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, such that $\pi(U^*) = 1$. In view of (48) and (47), we know $\text{supp}(U) \cap \tau\langle\alpha\rangle \neq \emptyset$. Thus, in view of Lemma 2.3, we can cyclically shift the terms of U^* until w.l.o.g. $U^*(1) \in \tau\langle\alpha\rangle$. In view of the formula (49) for $U^* = R^*$, we see that we can shift the position of a term x of U^* from $\langle\alpha\rangle$ while preserving that $\pi(U^*) = 1$ so long as we maintain the parity of the number of terms of U^* from $\tau\langle\alpha\rangle$ that follow to the right of x . In particular, we can put all terms of U^* from $\langle\alpha\rangle$ for which this number is odd into a consecutive block starting with the second term of U^* , while also putting all terms of U^* from $\langle\alpha\rangle$ for which this number is even into a consecutive block at the very end of U^* , and this will preserve that $\pi(U^*) = 1$. In other words, we may w.l.o.g. assume U^* has the form

$$U^* = (\tau\alpha^{x_1}) \cdot (\alpha^{y_1} \cdot \dots \cdot \alpha^{y_t}) \cdot (\tau\alpha^{x_2} \cdot \dots \cdot \tau\alpha^{x_{2w}}) \cdot (\alpha^{y'_1} \cdot \dots \cdot \alpha^{y'_{t'}}),$$

for some $t, t' \geq 0$ with

$$t + t' = |U_\alpha|, \quad 2w = |U_\tau| \geq 2, \quad \text{and} \quad x_i, y_i, y'_i \in [0, n-1].$$

Let $J' \subset [1, |U|]$ be those indices $j \in [1, |U|]$ such that $U^*(j) \in \tau\langle\alpha\rangle$, i.e.,

$$J' = \{1\} \cup [t+2, t+2w].$$

Now $T = U^*(I)$ for some $I \subset [1, |U|]$. Factor $T = T_\alpha \cdot T_\tau$ with $\text{supp}(T_\alpha) \subset \langle\alpha\rangle$ and $\text{supp}(T_\tau) \subset \tau\langle\alpha\rangle$. Since $\text{supp}(U^*(J')) \subset \tau\langle\alpha\rangle$, we see that T_α is disjoint from $U^*(J')$. For the remaining terms of T , we must have $T_\tau = (U^*(J'))(X)$ for some subset $X \subset [1, 2w]$. Let $X = X^+ \cup X^-$, where $X^+ \subset X$ is the subset of indices $x \in X$ with x even and $X^- \subset X$ is the subset of indices $x \in X$ with x odd. Consider an arbitrary term of T from $\tau\langle\alpha\rangle$, say $(U^*(J'))(x)$ with $x \in X \subset [1, 2w]$. If $x \in X^-$, then $(U^*(J'))(x)$ can be moved freely about in $(U^*(J'))(\{1, 2, \dots, 2w-1\})$ without changing that $\pi(U^*) = 1$. Likewise, if $x \in X^+$, then $(U^*(J'))(x)$ can be moved freely about in $(U^*(J'))(\{2, 4, \dots, 2w\})$ without changing that $\pi(U^*) = 1$. Consequently, we can w.l.o.g assume that X^- consists of the first $|X^-|$ elements from $\{1, 3, \dots, 2w-1\}$ and that X^+ consists of the first $|X^+|$ elements from $\{2, 4, \dots, 2w\}$. But this means that

$$T_\tau \mid U^*\left(\{1\} \cup [t+2, t+2|X|]\right).$$

As a result, setting

$$J := [t+1 + \max\{2|X|, 1\}, t+2w] \subset J' \setminus \{1\}$$

and recalling from the beginning of the paragraph that T_α is disjoint from $U^*(J')$, we find that $T \mid \left[U^*\left([1, |U|] \setminus J\right)\right]$. It remains to estimate $|J|$.

Since $|X| = |T_\tau| \leq |T| \leq n^+ - 1$ holds by hypothesis, it follows in view of (45) that

$$|J| = 2w - \max\{2|X|, 1\} = |U_\tau| - \max\{2|X|, 1\} \geq |U_\tau| - \max\{2|T|, 1\} \geq |U_\tau| - 2n^+ + 2. \quad (51)$$

From (48) and (47), we know

$$|U_\tau| = |U| - |U_\alpha| \geq (n + n^+ + 1) - (n^+ + n^- - 3) = n^+n^- - n^- + 4.$$

Combining this with (51) and making use of (45) and (46), we find that

$$|J| \geq n^+n^- - 2n^+ - n^- + 6 = 3n^- - 6 - n^- + 6 = 2n^-,$$

completing the proof of Claim A. \square

We will say that a subsequence $T \mid U$ is *good* if it has an ordering $T^* \in \mathcal{F}^*(G)$, so $[T^*] = T$, such that

$$T^* = y_1 \cdot z_1 \cdot \dots \cdot y_w \cdot z_w \cdot x_1 \cdot \dots \cdot x_v \quad (52)$$

with $v, w \geq 0$,

$$x_i \in \langle\alpha\rangle \setminus Z(G) \quad \text{for } i \in [1, v], \quad \text{and} \quad y_i, z_i \in \tau\langle\alpha\rangle \quad \text{and} \quad \iota(y_i) \not\equiv \iota(z_i) \pmod{p} \quad \text{for } i \in [1, w].$$

Furthermore, we define

$$\varphi(T^*) = (y_1 z_1) \cdot \dots \cdot (y_w z_w) \cdot x_1 \cdot \dots \cdot x_v \in \mathcal{F}^*(\langle\alpha\rangle) \quad \text{and} \quad \ell(T) = |\varphi(T^*)| = v + w. \quad (53)$$

We continue with the following claim.

Claim B. If $T \mid U$ is a good subsequence with $\ell(T) \geq n^+ - 1 = p - 1$, then $\pi(T)$ is a G' -coset.

Proof. Let $T^* \in \mathcal{F}^*(G)$ be an ordering from the definition of T notated as in (52) and (53). Since $\ell(T) \geq n^+ - 1 = p - 1$, it follows from (48) that $w \geq 1$. As remarked in Section 2, $\pi(T)$ is contained in a G' -coset. Therefore we need to show that $|\pi(T)| = |G'| = p$.

Since $w \geq 1$, it follows from (50) and the definition of \overline{g} that

$$|\pi(T)| = |\{0, \overline{x_1}\} + \dots + \{0, \overline{x_v}\} + \Sigma_w(\overline{T_\tau})|, \quad (54)$$

where $T_\tau \mid T$ is the subsequence of terms from $\tau\langle\alpha\rangle$. Note that $|T_\tau| = 2w$. Since T is good, we know $x_i \in \langle\alpha\rangle \setminus Z(G) = \langle\alpha\rangle \setminus \langle\alpha^p\rangle$ for $i \in [1, v]$, which means that $\overline{x_i} \neq 0$ for all $i \in [1, v]$. Consequently, since p is prime, we can apply the Cauchy-Davenport Theorem to $\{0, \overline{x_1}\} + \dots + \{0, \overline{x_v}\}$ to conclude

$$|\{0, \overline{x_1}\} + \dots + \{0, \overline{x_v}\}| \geq \min\{p, v + 1\}. \quad (55)$$

Since T is good, we have $\overline{y_i} \neq \overline{z_i}$ for $i \in [1, w]$, which together with the pigeonhole principle ensures that $h(\overline{T_\tau}) \leq w$. Consequently, since p is prime, we can apply Theorem 4.2 to $\Sigma_w(\overline{T_\tau})$ to conclude

$$|\Sigma_w(\overline{T_\tau})| \geq \min\{p, |T_\tau| - w + 1\} = \min\{p, w + 1\}. \quad (56)$$

Applying the Cauchy-Davenport Theorem to the 2-fold sumset $(\{0, \overline{x_1}\} + \dots + \{0, \overline{x_v}\}) + \Sigma_w(\overline{T_\tau})$, using (55) and (56), and recalling the case hypothesis $\ell(T) \geq p - 1$, it follows that

$$|(\{0, \overline{x_1}\} + \dots + \{0, \overline{x_v}\}) + \Sigma_w(\overline{T_\tau})| \geq \min\{p, v + 1 + w + 1 - 1\} = \min\{p, \ell(T) + 1\} = p.$$

Combining this with (54) completes the proof of Claim B. \square

Let $T \mid U$ be a good subsequence with $\ell(T) \geq 0$ maximal and let $T^* \in \mathcal{F}^*(G)$ be an ordering from the definition of T notated as in (52) and (53). We handle two cases.

Case 1: $\ell(T) \geq 2n^+ + n^- - 3$.

Recall the definition of $\varphi(T^*)$ given in (53). We first proceed to show that there is a good subsequence $T' \mid T$ with

$$\ell(T') \geq n^+ - 1, \quad \pi(T') \subset G', \quad T \cdot T'^{[-1]} \quad \text{a good subsequence,} \quad \text{and} \quad \ell(T \cdot T'^{[-1]}) \geq n^+ - 1. \quad (57)$$

To do so, it suffices, in view of the case hypothesis $\ell(T) = |\varphi(T^*)| \geq 2n^+ + n^- - 3$, to show that $[\phi_{G'}(\varphi(T^*))]$ has a product-one subsequence of length $\ell \in [n^+ - 1, n^+ - 2 + n^-]$. Note that

$$[\phi_{G'}(\varphi(T^*))] \in \mathcal{F}(\langle\alpha\rangle/G').$$

Thus, since $\ell(T) \geq n^+ - 2 + n^-$ holds by hypothesis, and since $d(\langle\alpha\rangle/G') + 1 \leq |\langle\alpha\rangle/G'| = n^-$ follows from Lemma 2.4, such a subsequence can be found simply by repeated application of the definition of $d(\langle\alpha\rangle/G')$ to $[\phi_{G'}(\varphi(T^*))]$. This establishes (57).

In view of (57) and Claim B, we have $\pi(T') = G'$. In particular, T' is a nontrivial, product-one subsequence of U . Thus Lemma 2.2 shows that $\pi(U \cdot T'^{[-1]}) \subset G'$. As a result, since $T \cdot T'^{[-1]} \mid U \cdot T'^{[-1]}$, it follows in view of (57) and Claim B that $\pi(U \cdot T'^{[-1]}) = G'$, so that $U \cdot T'^{[-1]}$ is also a product-one subsequence. But now $U = T' \cdot (U \cdot T'^{[-1]})$ is a factorization of U into 2 nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. This completes Case 1.

Case 2: $\ell(T) \leq 2n^+ + n^- - 4$.

In view of (48), we know $|U_\alpha \cdot U'_\alpha{}^{[-1]}| \leq n^- - 1$. We have

$$2(2n^+ + n^- - 4) + 1 \leq |U| - |U_\alpha \cdot U'_\alpha{}^{[-1]}|, \quad (58)$$

for if (58) failed, then $|U_\alpha \cdot U'_\alpha{}^{[-1]}| \leq n^- - 1$, (47), (45) and (46) would imply

$$0 > |U| - 4n^+ - 3n^- + 8 \geq n^+n^- - 3n^+ - 3n^- + 9 = (n^+ - 3)(n^- - 3) \geq 0,$$

which is a contradiction. In view of the maximality of $\ell(T)$, we must have $U'_\alpha \mid T$. Let $T_\tau = T \cdot U'_\alpha{}^{[-1]}$. Then, in view of the case hypothesis, it follows that $T_\tau \mid U_\tau$ is a good subsequence with

$$\ell(T_\tau) = \ell(T) - |U'_\alpha| \leq 2n^+ + n^- - |U'_\alpha| - 4 \quad \text{maximal subject to } T_\tau \mid U_\tau. \quad (59)$$

From (58), we deduce that

$$2(2n^+ + n^- - 4 - |U'_\alpha|) + 1 \leq |U| - |U_\alpha \cdot U'_\alpha{}^{[-1]}| - |U'_\alpha| = |U_\tau|. \quad (60)$$

Now $|U_\tau|$ must be even as remarked in the paragraph above (49), which means that the inequality in (60) must be strict:

$$2\ell := 2(2n^+ + n^- - |U'_\alpha| - 3) \leq |U_\tau|. \quad (61)$$

It is readily seen that a subsequence $R \mid U_\tau$ being a good is equivalent to \overline{R} having an $\frac{1}{2}|R|$ -setpartition with terms of as near equal a size as possible and $|R|$ even. In view of (59) and (48), we see that U_τ does not have a good subsequence $R \mid U_\tau$ with

$$\ell(R) = \frac{1}{2}|R| = \ell = 2n^+ + n^- - |U'_\alpha| - 3 \geq 1.$$

Thus applying Lemma 2.6 to $\overline{U_\tau}$ taking $\ell = n$, we conclude that either $2\ell > |U_\tau|$ or there exists a nonempty subset $X \subset G$ with $|X| \leq \lfloor \frac{\ell-1}{\ell} + 1 \rfloor = 1$ such that at least $|U_\tau| - \ell + 1$ terms of $\overline{U_\tau}$ are all from X . In view of (61), we see that the former is not possible, in which case the latter must hold, and with $|X| = 1$. In other words,

$$\mathbf{h}(\overline{U_\tau}) \geq |U_\tau| - \ell + 1. \quad (62)$$

Now (62) is equivalent to saying that there is some $x_0 \in [0, p-1]$ such that all but at most $\ell - 1$ terms of U_τ have the form $\tau\alpha^x$ with $x \equiv x_0 \pmod{p}$. However, since $p = n^+ = m^+ \mid r + 1$ follows from (29) in view of $\rho(P) = 1$ and the definition of m^+ , a short calculation shows that

$$H := \{\tau\alpha^x : x \in [0, n-1] \text{ and } x \equiv x_0 \pmod{p}\} \cup \{\alpha^y : y \equiv 0 \pmod{p}\} \leq G$$

is a subgroup of G having $|H| = 2n^-$. Indeed, $H = C_G(\tau\alpha^{x_0}) = \langle \alpha^p, \tau\alpha^{x_0} \rangle$, though we will not need this fact.

Let $U_H \mid U$ be the subsequence of U with terms from H . In view of the two previous paragraphs, we see that (62) is equivalent to saying

$$|U \cdot U_H{}^{[-1]}| \leq |U'_\alpha| + \ell - 1 = 2n^+ + n^- - 4. \quad (63)$$

As a result, we have

$$|U_H| \geq 2n^- + n^+ - 1, \quad (64)$$

for if (64) failed, then combining this with (63) and (47) would yield

$$n^+n^- + n^+ + 1 \leq |U| = |U_H| + |U \cdot U_H{}^{[-1]}| \leq 3n^+ + 3n^- - 6,$$

and then rearranging the above inequality and applying (45) and (46) yields the contradiction

$$0 \geq n^+ n^- - 2n^+ - 3n^- + 7 \geq 3n^- - 6 - 3n^- + 7 = 1.$$

Let x be a term from $U \cdot U_H^{[-1]}$. If $x \in \langle \alpha \rangle$, then $x \in \text{supp}(U'_\alpha)$ and x can be included in a good sequence. On the other hand, if $x \in \tau\langle \alpha \rangle$, then x can be paired with any term from U_H lying in $\tau\langle \alpha \rangle$ and thereby included in a good sequence. In particular, if we know that there are at least $t \geq 0$ terms of U from $H \cap \tau\langle \alpha \rangle$, then U possesses a good subsequence $R \mid U$ with $\ell(R) = \min\{t, |U \cdot U_H^{[-1]}|\}$.

With these key facts finally established, we are now ready to finish the proof, which we do in 2 short subcases.

Case 2.1. $|U \cdot U_H^{[-1]}| \geq n^+ - 1$.

Recall that $H \cap \langle \alpha \rangle = \langle \alpha^p \rangle = Z(G)$ and that $U_\alpha \cdot U'_\alpha^{[-1]}$ is the subsequence of U consisting of all terms from $Z(G)$. Thus, in view of (64) and (48), we can find a subsequence $U'_H \mid U_H$ with $U_\alpha \cdot U'_\alpha^{[-1]} \mid U'_H$ and $|U'_H| = 2n^-$. Since $U_\alpha \cdot U'_\alpha^{[-1]}$ is the subsequence of U consisting of all terms from $Z(G) = H \cap \langle \alpha \rangle$, since $U_\alpha \cdot U'_\alpha^{[-1]} \mid U'_H$ and since $\text{supp}(U_H) \subset H$, we see that

$$\text{supp}(U_H \cdot U'_H^{[-1]}) \subset H \cap \tau\langle \alpha \rangle. \quad (65)$$

Since $|U'_H| = 2n^- = |H|$, applying Lemma 2.4 to U'_H yields a nontrivial, product-one subsequence $R \mid U'_H$. From Lemma 2.2, it follows that

$$\pi(U \cdot R^{[-1]}) \subset G'. \quad (66)$$

Since $R \mid U'_H$, we have

$$U \cdot U'_H^{[-1]} \mid U \cdot R^{[-1]}. \quad (67)$$

Since $R \mid U'_H$ and $U'_H \mid U_H$, we have

$$U \cdot U_H^{[-1]} \mid U \cdot R^{[-1]}. \quad (68)$$

From (64), we find that

$$|U_H \cdot U'_H^{[-1]}| \geq 2n^- + n^+ - 1 - |U'_H| = n^+ - 1.$$

Consequently, it follows in view of (65) and (67) that there are at least $n^+ - 1$ terms of $U \cdot R^{[-1]}$ from $H \cap \tau\langle \alpha \rangle$. Combining this with (68) and applying the argument given just above Case 2.1, it follows that $U \cdot R^{[-1]}$ contains a good subsequence $T \mid U \cdot R^{[-1]}$ with $\ell(T) \geq \min\{n^+ - 1, |U \cdot U_H^{[-1]}|\} \geq n^+ - 1$, where the latter inequality follows in view of the subcase hypothesis. But now, in view of (66), we can apply Claim B to find that $\pi(U \cdot R^{[-1]})$ is not just contained in G' , but must be equal to G' , so $\pi(U \cdot R^{[-1]}) = G'$. Hence $U = R \cdot (U \cdot R^{[-1]})$ is a factorization of U into 2 nontrivial, product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom.

Case 2.2. $|U \cdot U_H^{[-1]}| \leq n^+ - 2$.

In this case, we can apply Claim A using $T = U \cdot U_H^{[-1]}$ to find an ordering of U , say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, and an interval $J \subset [1, |U|]$ such that

$$\pi(U^*) = 1, \quad U \cdot U_H^{[-1]} \mid U^*([1, |U|] \setminus J) \quad \text{and} \quad |J| \geq |H| = 2n^-.$$

In view of $U \cdot U_H^{[-1]} \mid U^*([1, |U|] \setminus J)$, we have $U^*(J) \mid U_H$. Thus $U^*(J) \in \mathcal{F}(H)$ with $|U^*(J)| = |J| \geq 2n^- = |H|$. As a result, applying Lemma 2.4 yields a nontrivial, consecutive, product-one subsequence R^* in $U^*(J)$ with $|R^*| \leq 2n^-$. Since $U^*(J) \mid U^*$ is also consecutive (as $J \subset [1, |U|]$ is an interval), this

means that $R^* \mid U^*$ is a nontrivial, consecutive, product-one sequence in U^* with $U = [U^*] \in \mathcal{A}(G)$ an atom, in which case Lemma 2.1 ensures that $R^* = U^*$. But then (47) and (45) give

$$2n^- \geq |R^*| = |U^*| = |U| \geq n^+n^- + n^+ + 1 \geq 3n^- + 4,$$

which is a proof concluding contradiction. \square

ACKNOWLEDGEMENT

We wish to thank the referee for their suggestions, particularly the idea leading to Theorem 3.2, without which the paper would have remained much more limited in scope.

REFERENCES

- [1] P. Baginski and S.T. Chapman, *Factorizations of algebraic integers, block monoids, and additive number theory*, Am. Math. Mon. **118** (2011), 901 – 920.
- [2] J. Bass, *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*, J. Number Theory **126** (2007), 217 – 236.
- [3] Y. Berkovich, *Groups of prime power order, vol I*, Expositions in Mathematics, vol. 46, de Gruyter, 2008.
- [4] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspeich, *On some developments of the Erdős-Ginzburg-Ziv Theorem II*, Acta Arith. **110** (2003), 173 – 184.
- [5] Y. Caro, *Zero-sum problems - a survey*, Discrete Math. **152** (1996), 93 – 113.
- [6] M. DeVos, L. Goddyn, and B. Mohar, *A generalization of Kneser's addition theorem*, Adv. Math. **220** (2009), 1531 – 1548.
- [7] A. Facchini, *Krull monoids and their application in module theory*, Algebras, Rings and their Representations (A. Facchini, K. Fuller, C. M. Ringel, and C. Santa-Clara, eds.), World Scientific, 2006, pp. 53 – 71.
- [8] A. Facchini, W. Hassler, L. Klingler, and R. Wiegand, *Direct-sum decompositions over one-dimensional Cohen-Macaulay local rings*, Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 153 – 168.
- [9] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.
- [10] W. Gao and Yuanlin Li, *The Erdős-Ginzburg-Ziv theorem for finite solvable groups*, J. Pure Appl. Algebra **214** (2010), 898 – 909.
- [11] W. Gao and Zaiping Lu, *The Erdős-Ginzburg-Ziv theorem for dihedral groups*, J. Pure Appl. Algebra **212** (2008), 311 – 319.
- [12] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.
- [13] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: a survey*, Multiplicative Ideal Theory in Commutative Algebra (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 207 – 226.
- [14] ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [15] A. Geroldinger and M.D. Neusel, *On the interplay between invariant theory and zero-sum theory*, manuscript.
- [16] D.J. Grynkiewicz, *The large Davenport constant II: General upper bounds*, manuscript.
- [17] ———, *Structural Additive Theory*, to appear, 2013.
- [18] F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.
- [19] ———, *Non-unique factorizations of algebraic integers*, Funct. Approximatio, Comment. Math. **39** (2008), 49 – 60.
- [20] D.L. Johnson, *Presentations of Groups*, Student Texts, vol. 15, London Math. Soc., 1990.
- [21] G.A. Jones, Jinho Kwak, and Mingyao Xu, *Finite Group Theory for Combinatorists*, Chapman & Hall/CRC, to appear.
- [22] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319 – 330.
- [23] M. D. Neusel, *Degree bounds – an invitation to postmodern invariant theory*, Topology Appl. **154** (2007), 792 – 814.

- [24] ———, *Invariant Theory*, Student Mathematical Library, vol. 36, AMS, 2007.
- [25] M. D. Neusel and L. Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs, vol. 94, AMS, 2002.
- [26] J.E. Olson and E.T. White, *Sums from a sequence of group elements*, Number Theory and Algebra (H. Zassenhaus, ed.), Academic Press, 1977, pp. 215 – 222.
- [27] K. Rogers, *A combinatorial problem in abelian groups*, Proc. Camb. Philos. Soc. **59** (1963), 559 – 562.
- [28] W.A. Schmid, *Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report*, Number Theory and Applications: Proceedings of the International Conferences on Number Theory and Cryptography (S.D. Adhikari and B. Ramakrishnan, eds.), Hindustan Book Agency, 2009, pp. 189 – 212.
- [29] Guoqing Wang and Weidong Gao, *Davenport constants for semigroups*, Semigroup Forum **76** (2008), 234 – 238.
- [30] H. Zassenhaus, *The theory of groups, 2nd ed.*, Vandenhoeck & Ruprecht, Göttingen, 1956.
- [31] J. Zhuang and W. Gao, *Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index*, Eur. J. Comb. **26** (2005), 1053 – 1059.

INSTITUT FÜR MATHEMATIK UND WISSENSCHAFTLICHES RECHNEN, KARL-FRANZENS-UNIVERSITÄT GRAZ, HEINRICHSTRASSE
36, 8010 GRAZ, AUSTRIA

E-mail address: `alfred.geroldinger@uni-graz.at`, `diambri@hotmail.com`